ARMY RESEARCH LABORATORY

A Study of Packet Routing in Mobile Radio Networks

by Madhavi Subbarao
and Ramaswamy Murali

ARL-CR-337 January 1998

prepared by

Department of Electrical and Computer Engineering
The Johns Hopkins University
3400 North Charles Street
Baltimore, MD 21218

under contract

DAAL03-91-C-0034

Army Research Laboratory
Aberdeen Proving Ground, MD 21005-5067

ARL-CR-337 **January 1998**

A Study of Packet Routing in Mobile Radio Networks

Madhavi Subbarao, Ramaswamy Murali
The Johns Hopkins University

prepared by

Department of Electrical and Computer Engineering
The Johns Hopkins University
3400 North Charles Street
Baltimore, MD 21218

under contract

DAAL03-91-C-0034

Abstract

This study is concerned with mobile packet radio networks. These networks are of importance in the context of tactical battlefield communications, where decentralized operation and antijam capability are desirable network attributes. The objective of this study is to conduct and document a survey of the known and available results on techniques for routing information through packet radio networks. We focus on issues that reside within the first (lower) three layers of the seven-layer open system interconnection (OSI) network architecture model. Consequently, a greater emphasis is placed on issues, such as network connectivity, media access, and routing. Where available, performance evaluation methods are detailed. Finally, we present examples of commercial, state-of-the-art wireless data networks and discuss some open problems for further study.

Acknowledgments

We would like to express our appreciation to Dr. A. Brinton Cooper, III for giving us the opportunity to work on this study for the U.S. Army Research Laboratory (ARL). We are grateful for his insightful suggestions and comments throughout the course of this project. On several occasions, Dr. Cooper provided us with useful references and preprints of journal articles. We greatly benefitted from his experience and knowledge.

We are also indebted to Dr. Brian L. Hughes for his support and encouragement throughout the study. As our advisor and mentor, he has always taken great interest in our work and progress. His guidance has been truly invaluable. We are extremely thankful for his careful review of this manuscript.

This work was supported by ARL (Dr. A. Brinton Cooper, III) under the auspices of the U.S. Army Research Office Scientific Services Program administered by Battelle (Delivery Order 1420, Contract No. DAAL03-91-C-0034).

Intentionally Left Blank

Contents

List of Figures

Intentionally Left Blank

1. Introduction

A *mobile packet radio network* consists of a collection of movable terminals (or nodes) distributed over a wide geographical area and the radio links which connect them. Information is transmitted between terminals in the form of discrete blocks of data called *packets.* Each terminal has packet-switching capabilities and may represent a transmitter, receiver, or relay station. These networks typically lack a fixed infrastructure: terminals are mobile, there is no central hub or controller, and thus there is no fixed network topology. Examples of such networks include the U.S. Army's Single Channel Ground to Airborne Radio System (SINCGARS) and the U.S. Navy's High-Frequency (HF) Intra Task Force (ITF) network.

Packet radio networks must contend with a difficult and variable communications environment. First, packet transmissions are plagued by the usual problems of radio communication, which include propagation path loss, signal multipath and fading, and thermal noise. Second, these effects vary with terminal movement, which also induces Doppler spreading in the frequency of the transmitted signal. Finally, transmissions from neighboring terminals and hostile jammers may contribute additional interference.

To communicate under these harsh conditions, the network protocols must perform several basic functions. First, the protocols must establish and maintain radio connectivity between neighboring terminals, whenever feasible. Second, they must ensure reliable transmission of data packets between connected terminals. Third, the protocols should build and maintain routing tables to guide packets through the network from the source terminal to the destination.

From a communication viewpoint, the following features are desirable in protocols for mobile packet radio networks:

- The dynamic nature of the network mandates frequent topological restructuring; hence,

the network should be *self-organizing* and *adaptive*.

- The network should provide communication between any pair of nodes, at all times.

- The network should have a *decentralized* structure, i.e., each terminal should base its actions on locally gathered information. Moreover, the network should be able to cope with arriving and departing terminals, and it should degrade gracefully when terminals fail.

- The network should be robust against jamming and multiuser interference, multipath fading, and propagation path loss.

1.1 Objective of the Study

This report comprehensively surveys the literature on routing in mobile packet radio networks. The focus is on dynamic networks with changing topologies and varying link qualities. Particular goals of the study include:

- discussing techniques for ensuring connectivity among mobile terminals,

- examining various random *channel access*, *link scheduling*, and *channel signaling* methods,

- examining *adaptive* multihop routing algorithms,

- addressing the role of network congestion on the performance of routing algorithms, and

- describing the fading channel and packet radio network models used.

1.2 Design Issues in Mobile Packet Radio Networks

There are many fundamental issues that arise in designing a mobile packet radio network. In this study, we focus on those that reside within the lower three layers of the seven-layer open systems interconnection (OSI) network architecture model. We briefly discuss these issues in the following paragraphs.

(1) *Network Connectivity*: In a decentralized mobile packet radio environment, the network is subject to changes in connectivity. These changes are initiated by many factors, including terminal motion, jamming, terrain changes, and equipment malfunction. Consequently, in the absence of a central controller, how do mobile terminals establish and maintain connectivity at all times? *Distributed* algorithms are necessary that either (a) construct a *backbone* network, or (b) discover nodal connectivities as part of the packet routing protocol. (An emerging trend in the literature is to consider routing algorithms in which network connectivity is determined in the process of routing packets.)

(2) *Media Access*: Once connectivities between terminals are known, how do terminals access the common radio channel? Since the radio channel is a *multiaccess broadcast* resource that is shared by many contending users, action taken by a node affects actions taken by neighboring nodes in the network. Consequently, a *channel access* protocol is needed to efficiently share the radio channel. Moreover, a *channel signaling* technique, to determine the mode of data transmission (e.g., narrowband or spread-spectrum), and a *link scheduling* algorithm, to provide a schedule for enabling links in networks with a backbone, are also needed. What are the commonly used methods for channel access, channel signaling, and link scheduling?

(3) *Routing*: Given network connectivity and media access methods, how are packets routed through the network from source to destination? In many mobile packet radio networks, the routing problem is of a *multihop* nature, as packets may pass through intermediate (relay) nodes before reaching their destination. More precisely then, how are routing tables constructed and maintained when network topology is changing?

(4) *Modeling and Performance Evaluation*: Finally, what are the important performance measures for a mobile packet radio network? Standard global performance measures include *throughput*, *delay*, and *stability*. For routing protocols, the worst-case computational complexity is also an important measure. What are the analytically tractable models that exist to emulate the dynamic nature of a mobile packet radio network (e.g., multipath fading and varying link quality)?

1.3 Organization of the report

The report is organized as follows. Section 2 discusses distributed algorithms for ensuring network connectivity in a mobile radio environment. (The Appendix contains a brief overview of the main characteristics of radio propagation.) In particular, section 2 discusses in detail the *linked-cluster architecture* algorithm used in the Navy's HF ITF network [1], which constructs and adaptively maintains a backbone network for communication between nodes. Section 3 first outlines the distinctive characteristics of the radio channel and then discusses various channel signaling, channel access, and link scheduling methods. Performance evaluations of channel access and channel signaling methods for both single-hop and multihop networks are then presented. Section 4 examines protocols for packet routing. Protocol performance evaluations are included. Section 5 discusses examples of commercial wireless data networks. Finally, section 6, presents our concluding remarks and mentions some open problems for further study.

2. Network Connectivity

This section is concerned with issues that reside within the *physical* layer of the OSI model. The fundamental problem in this layer is to provide the means by which existing connectivities among the nodes can be discovered. This problem is particularly complicated in the case of a packet radio network since typically it has no *a priori* structure and hence,

there are no assumptions on a connectivity structure or on role assignments to nodes for the purpose of network control [1]. Also, in a mobile radio environment, changes in network connectivity can be brought about by many factors, such as the presence of a jammer, propagation path loss, fading due to multipath, and terrain changes.

One approach to ensure complete network connectivity involves the use of a *distributed* network organization algorithm to determine which nodes are connected and to dynamically assign roles to nodes for network control. In the following paragraphs, we describe one such algorithm. Alternatively, in the recent literature, there is a discernible trend toward determining network connectivities as part of the process of routing packets. Such algorithms are addressed in section 4.

For the network organization problem discussed next, it is assumed that the network consists of mobile nodes, geographically dispersed over distances which may be beyond the line of sight (LOS), and links that connect these nodes. A node has no *a priori* knowledge of the locations of the other nodes, the connectivities of the network, or even its own neighbors. The only knowledge available to a network member (i.e., a node) is the set of possible network members, each having a unique identity (unique ID number).

An example of an algorithm used to determine network connectivity is the *Linked Cluster Algorithm* (LCA) developed in a series of papers by Ephremides, Wieselthier, and Baker [1, 2, 3, 4, 5]. The algorithm was specifically developed for the HF ITF Network, a network designed to provide extended line of sight (ELOS) (50 to 1,000 km) communication for a Naval task force. Ample documentation of the LCA can also be found in Baker, Ephremides, and Flynn [6].

The LCA permits the nodes to discover each other and ultimately yields an overall network topology that facilitates network operations, e.g, message broadcasting. The interconnection structure that results from this algorithm consists of interconnected clusters of nodes, hence the name LCA. The goals of the algorithm are that, as links are discovered, a structure

results that will permit:

(1) communication between any pair of nodes by forming *bidirectional* (two-way) links,

(2) network-wide broadcasts,

(3) avoidance of the "hidden-terminal" problem [7], and

(4) robust recovery from node or link losses and other topological changes.

Furthermore, the process of organization is fully distributed.

In the LCA, nodes can assume one of three roles: a node may be a *clusterhead*, a *gateway*, or an *ordinary node*. Each node is associated with a designated clusterhead, called its *own clusterhead*. A node may also be within communication range of other clusterhead nodes. The clusterhead can assume various responsibilities; for instance, it *may* act as a local controller for all the nodes in its cluster. An example is when intracluster communication is controlled by the clusterhead acting either as a polling agent for noncontention communication, or as a "busy-tone" emitter in a contention-based mode. The LCA is designed so that two clusterheads are never directly connected to each other. Consequently, gateways are used to provide communication between two clusters, thereby producing overall network connectivity. The clusterheads, gateway nodes, and the links that interconnect them form the *backbone* network (see Figure 1).

The LCA consists of two steps: cluster formation and cluster linkage, which are, in turn, divided into a *computation part* and a *communication part*.

(1) *Computation (cluster formation and linkage):* For simplicity, we explain the algorithm in the context of an example in which the entire network topology is known to a central controller. The communication range is a fixed constant R for all nodes. (The

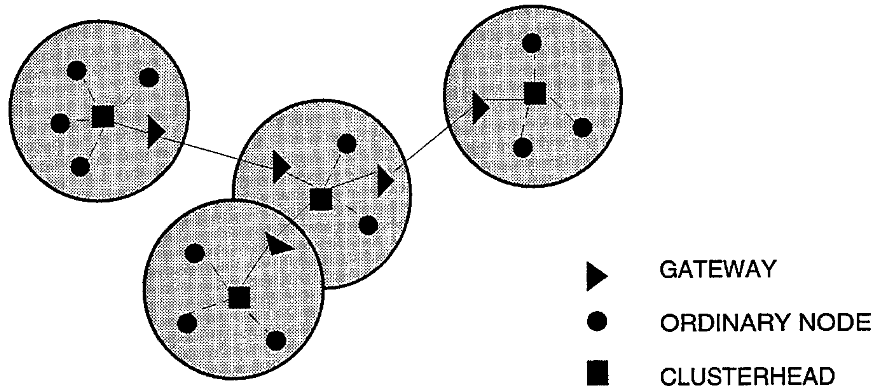


Figure 1: Example of linked-cluster network organization of a mobile packet radio network.

distributed implementation of the algorithm without a central controller and without assuming a fixed communication range R is described in the communication part of the algorithm.) The central controller arbitrarily selects a node, say node 1, to be a clusterhead. It then draws a circle of radius R around that node and declares all nodes within that circle to belong to the first cluster with node 1 as their *own* clusterhead. From the remaining nodes not in the first cluster, the controller chooses the node with the lowest ID number to be the next clusterhead. The central controller draws a circle of radius R around the new clusterhead and declares all nodes captured in this circle to be members of the second cluster. However, only the nodes which are not also in the first cluster are assigned the new clusterhead as their *own* clusterhead. The process is repeated until all nodes belong to at least *one* cluster.

After clusterheads have been determined, gateways must be chosen to provide inter-cluster communication. There are two cases, namely, overlapping clusters or adjacent, nonoverlapping clusters, as shown in Figure 2. In the nonoverlapping case, a pair of gateways is needed, i.e., one from each cluster. Regardless of the case, there is an unambiguous subset of nodes from which gateways can be selected. For the overlapping case, the node in the intersection of the two clusters with the lowest ID number can be selected. For the nonoverlapping case, the pair of nodes whose sum of ID numbers is the lowest can be chosen to be gateways. (These chosen nodes must be in transmission range of each other.) Further details on gateway selection can be found in

Baker, Ephremides, and Wieselthier; Baker and Ephremides; and Baker, Ephremides, and Flynn [4, 5, 6].

Note that the previous cluster formation process requires:

(a) knowledge of each node's bidirectional connectivities to neighboring nodes,

(b) a rule for selecting a clusterhead from a set of candidate nodes,

(c) specification of the sequence in which clusters are formed, and

(d) a rule for gateway selection from a group of candidate nodes.

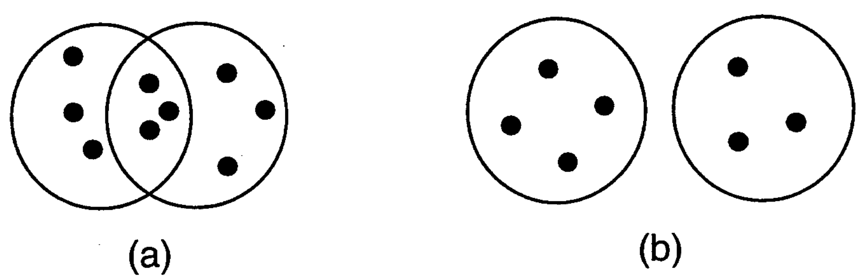


Figure 2: Two cases in linked cluster algorithm: (a) overlapping clusters, and (b) nonoverlapping clusters.

(2) *Communication (database collection for distributed implementations):* A process of probing is used for each node to discover who its neighbors are. A probe message is broadcast, and every node that hears it sends an acknowledgment back to the probing node. A strategy to implement the probing process is to set up two time-division multiple access (TDMA) frames for controlling the transmission of probe and acknowledgment messages. Each node is assigned its own transmission time once in each frame. In the first frame, each node broadcasts its probe message, e.g., announcing its identity, and also acknowledges the receipt of previously transmitted probe messages from other nodes that it has heard. The acknowledgments can be done by announcing the

ID numbers of those nodes it has heard. During frame 2, each node acknowledges any probe messages that it has received since its own frame 1 transmission. As a result of this probing process, each node discovers who it is bidirectionally connected with Baker, Ephremides, and Wieselthier; Baker and Ephremides; and Baker, Ephremides, and Flynn [4, 5, 6]. Only bidirectional links are used in the formation of the backbone network.

Just prior to its frame 2 transmission, each node has obtained the information it needs to implement the cluster formation step in the linked cluster architecture. In its frame 2 transmission, each node includes an announcement of the decision to become a clusterhead, if, in fact, the node has so decided. This decision is revealed by the node including the ID of its own clusterhead in its frame 2 transmission. Each node selects, as its *own* clusterhead, the node with the lowest ID to which it is bidirectionally connected. A node decides to become a clusterhead if, by its frame 2 transmission, it has not already heard from a clusterhead to which it is bidirectionally connected. Consequently, node 1 always becomes a clusterhead, and node i, for $i > 1$, becomes a clusterhead if it is not bidirectionally connected to a clusterhead whose ID is less than i.

An advantage of using a TDMA-based probing procedure is its contention-free nature and the knowledge of the duration of the organization period. Network-wide synchronization at the slot level is easy to maintain, since the slot duration is much greater than the anticipated timing uncertainties throughout the network. Moreover, in contention-free systems, spread-spectrum synchronization is easier to acquire than in systems in which contention is permitted. However, a disadvantage of the TDMA structure is that when the number of nodes is large, the organizational period becomes long. For larger networks, therefore, it may be necessary to use alternative methods for maintaining linked-cluster networks. Possible alternatives may be to proceed asynchronously with a contention-based protocol or to allow a limited subset of nodes to participate in the formation of a backbone network.

A node must address two issues when deciding whether to serve as a gateway: identifying the clusters for which it can serve as a gateway, and identifying all other nodes that can do the same. For the nodes that are inside cluster intersections, the selection can be made unambiguously, based on the information that has been gathered in frame 2. In the case of nonoverlapping adjacent cluster configurations, the algorithms described in Baker, Ephremides, and Wieselthier; Baker and Ephremides; and Baker, Ephremides, and Flynn [4, 5, 6] occasionally yield more than one pair of gateways linking the clusters or an additional "half-pair," (one node in one cluster that decides to serve as a gateway along with a node from the other cluster that does not decide the same). These superfluous gateways are not harmful, and their inclusion is at worst a nuisance.

Note that the chosen order of cluster formation results in a set of clusters which is not optimized in any way. For example, it does not achieve the minimum number of clusters; it is not known whether such a goal is, in fact, desirable. It does, however, produce a connected network whenever the required link connectivities are present. Other than node 1, it is also not known *a priori* which nodes will become clusterheads. If it is desirable that certain nodes should become clusterheads, then they can be assigned low ID numbers.

The communication range of HF groundwaves varies considerably as frequency is varied over the HF band. The linked cluster architecture takes advantage of this variation in the HF band by partitioning the HF band into several subbands, each with a bandwidth of a few MHz over which the communication range for groundwaves is approximately constant. The LCA is then run separately for each subband, resulting in a set of overlaid connectivity maps, which give rise to a set of simultaneously operating networks. At most, one of these networks will reorganize itself at any time, while the remaining networks maintain communication using their most recently derived network structure.

In addition, two more observations should be made.

(1) There need not be any assumptions made concerning the communication range, e.g., it need not be uniform or symmetric. The algorithm discovers within each subband the nodes which can be heard by a given node.

(2) The algorithm is inherently robust. For example, if a probing message is not received because of a deep fade or a local jammer, that link is not included in the backbone network. The loss of a potential connectivity during the network reorganization does not hinder the network, and later use of that link is possible, although not for backbone network communication.

3. Media Access

This section focuses on issues that reside within layer 2 of the OSI model. In traditional wireline networks, this layer is also called the *data link control* (DLC) layer. However, since packet radio networks possess characteristics that are fundamentally different from wire-based networks, there is a need for an additional sublayer (within layer 2) called *media access control* (MAC). Our concern here shall be on those problems that arise in the MAC sublayer.

This section is divided into two main parts. In the first section, we comment on the important differences between packet radio and wire-based communications. This is followed by a discussion of various techniques used for data transmission over packet radio channels. The second part of this section is concerned with the modeling and performance evaluation of packet radio networks.

3.1 Data Transmission

Packet radio communications are fundamentally different than traditional point-to-point, wire-based networks. The following are three important differences:

(1) While in a point-to-point network, each link constitutes a separate communication resource; in a packet radio network, there is a common radio channel over which terminals attempt data transmission. Consequently, efficient use of the available RF bandwidth becomes an important design issue.

(2) Due to the nature of wave propagation in mobile radio channels, the quality of individual links can vary widely. Contributing factors to link quality include the length of the link, changes in terrain, antenna type and orientation, and multipath fading. As a result, the connectivity between nodes is not a deterministic function, as in point-to-point, wire-based networks.

(3) The radio channel is a *multiaccess broadcast* resource; within a certain locality, terminals must share a common channel. Hence, all transmissions can be heard by multiple terminals. The success of a transmission initiated by a node depends not only on the quality of the link between the node and its intended receiver but also on the transmission activity of neighboring nodes and the state (transmit or receive mode) of the intended destination node.

The previously listed characteristics of a packet radio channel mandate the need for using efficient methods for medium access. Two approaches can be used: (1) for networks with established connectivities (e.g., through the use of the LCA algorithm), a *link scheduling* algorithm can be used for activation of links, and (2) for other networks, a *channel access* protocol can be used, which dictates when individual nodes may access the channel.

Apart from the use of a link scheduling algorithm and/or a channel access protocol, terminals must employ one of two standard *channel signaling* approaches: *narrow-band* or *spread-spectrum*. Notably, these two methods result in different *capture effects* and conditions for successful reception of a transmitted packet at a receiver. Capture refers to the ability of a receiving terminal to lock on to and successfully decode a single packet correctly when many (time-overlapping) packet transmissions are addressed to it.

In the remainder of this section, we first describe the two channel signaling approaches and corresponding capture effects. We then discuss various channel access protocols and link scheduling algorithms.

3.1.1 Channel Signaling and Capture

As mentioned earlier, there are two types of channel signaling methods: *narrow-band* and *spread-spectrum*. In narrow-band signaling, data bits are modulated directly onto the carrier; thus, overlap at a receiver of two packets with about the same signal power will typically result in destruction of both packets. However, if the signals are of different power, then the stronger packet may be received correctly while the weaker packet is lost. This is referred to as *power capture*, and sometimes depends on timing (e.g., a weak signal could tie up the synchronization circuit of the receiver). If all links in the network are of the same quality, then the possibility of power capture is removed. The network is then said to operate in *zero-capture mode*, where the overlap of two or more packets at a receiver results in the loss of all packets.

Spread-spectrum refers to signaling schemes in which the frequency spectrum of the information signal is *spread* out over a much larger bandwidth prior to transmission, and the received signal is *de-spread* to recover the information. Thus, spread-spectrum signaling uses a much wider bandwidth than narrow-band schemes for the same data rate [8]. Extensive treatment of spread spectrum signaling can be found in Dixon; Holmes; Simon et al.; and Special Issue on Spread Spectrum [9, 10, 11, 12]. The key motivation behind spread-spectrum signaling is to reduce the harmful effect of interference signals on system performance. The two most commonly used forms of spread-spectrum are *direct sequence pseudo-noise* (PN) modulation, and *frequency hopping* (FH). Direct sequence is a system in which the carrier undergoes rapid phase changes that are governed by a *spreading code*. The spreading code usually has a bandwidth which is much greater than necessary to transmit the data. In FH spread spectrum, the FH carrier "hops" over a wide frequency band deter-

mined by the spreading code. In FH systems, the spreading code is also referred to as the *frequency-hopping pattern.*

Spread-spectrum signaling offers resistance to hostile interference, such as jamming. Other advantages include:

(1) *Anti-multipath:* This capability refers to the ability to communicate reliably over a link which has multiple transmission paths. On some radio channels, a signal may destructively interfere with delayed versions of itself arriving by alternate paths (e.g., due to atmospheric reflection). This phenomenon, known as *multipath*, can cause severe fading in the intensity of the received signal. The effect of multipath interference can be reduced by spread-spectrum signaling.

(2) *Low probability of intercept:* The power per unit bandwidth (energy density) of the transmitted signal is reduced by spreading the signal power over a large bandwidth. This spreading of the signal makes it difficult for an unauthorized user to intercept (or detect) the presence of the signal. Thus, spread-spectrum signaling is often used in the design of low probability of intercept (LPI) or low probability of detection (LPD) communication systems [13].

(3) *Ranging:* Spread-spectrum signals can be used for accurate determination of position location. The distance to a target is proportional to the time taken by the signal for a round-trip to the target. The large bandwidth of spread-spectrum signals allows accurate measurement of distance, since the error in measurement is inversely proportional to the bandwidth of the transmitted signal.

(4) *Multiple-access:* Spread-spectrum signaling can be used to share the same frequency spectrum among many users. Each user is provided with a unique *spreading code* for determining the spreading of the information signal. Consequently, users gain a measure of privacy from other users as well as from interference due to the transmissions

of other users. This multiple-access technique is referred to as *code-division multiple-access* (CDMA).

(5) *Time capture:* Time capture refers to the ability of an idle receiver to successfully receive a packet with a given spreading code, despite the presence of other time-overlapping transmissions with the same or other codes.

The choice of the spread-spectrum code for a particular transmission has a strong affect on the probability of success of that transmission. For many spread-spectrum systems, it is possible to change the spread-spectrum code from one transmission to another. *Spread-spectrum transmission protocols* are the rules that determine the selection of the spreading code to be used in a packet transmission. This selection can be dictated by the identity of the intended receiver or receivers, the identity of the transmitter, the time of day, the starting time for the transmission, the priority assigned to the message, etc.

In a practical network, transmission of packets is asynchronous, and hence each packet transmission must be preceded by the transmission of a *preamble* that the receivers use to acquire bit synchronization. The preamble typically contains the intended destination, the identity of the source node, and a known *synchronization code* with strong *autocorrelation* properties that are used throughout the network. (Correlation is a matching process; *auto-correlation* is the matching of a signal with a delayed version of itself. The autocorrelation function provides a measure of how closely a signal matches a copy of itself as the copy is shifted in time [13].)

The synchronization code is typically chosen to be *orthogonal* to the spreading codes. To receive a packet successfully, an idle receiver must first successfully detect the preamble. This process is complicated by the presence of other preambles due to overlapping packets from other users.

A packet radio network employing a *receiver-oriented* spread-spectrum transmission pro-

tocol can reduce the errors due to overlapping preambles. In this protocol, each receiver is assigned a distinct synchronization code, and transmitters must use the code assigned to the receiver with which they wish to communicate in their preambles. Consequently, a receiver will detect only the preambles of those packets intended for it. All other transmissions will appear as background noise. The performance of this protocol depends on the timing mechanism for generating the spreading code, the time offsets between different packets that are transmitted to the same receiver, and the energy level of the background noise due to other transmissions in the network. Having successfully detected the preamble of an incoming packet, a receiver is then synchronized with the transmitter and may demodulate the data portion of the acquired packet.

Once a packet is acquired by a receiver, it is important that future overlapping packets do not interfere with the rest of the transmission. The conditions for a success are dependent not only on the PN spreading code used, but also on the set of active links and their signal strengths. There are several cases that are of particular importance. Consider the scheme in which a *fixed PN spread-spectrum code* is used which is identical for each bit transmitted throughout the network. An overlapping packet would then only interfere with an acquired packet when its autocorrelation peaks coincide with those of the earlier packet. Hence, there is a vulnerable period of a few *chip* durations for each bit during which the arrival of a new packet would cause total loss. (The basic time unit of the spread-spectrum code is referred to as a *chip* for both frequency-hopping and direct-sequence spread spectrum.) However, since the vulnerable period for a packet is small compared to its entire transmission time, the capture effect becomes important. This case is referred to as the *space-and-bit-homogeneous code assignment.*

The assignment of distinct orthogonal spreading codes to different receivers reduces the effect of overlapping packets. This mode also reduces the amount of traffic that interferes with a packet transmitted to a receiver, since only the traffic which is destined for that particular receiver is relevant. This scheme is referred to as the *receiver-directed bit-homogeneous code assignment.*

By using a spreading code that varies on a bit-by-bit basis and equipping the receiver with a programmable matched filter which follows the code as it varies, it is feasible to eliminate interference from overlapping packets. An overlapping packet will not interfere with an acquired packet, if the code does not repeat during the transmission of the longest packet. This is manifest in the fact that the overlapping packet would not produce any autocorrelation peak during the entire reception of the earlier packet. If all codes are orthogonal and background noise is negligible, this coding scheme achieves *perfect capture* and correct reception is guaranteed once the packet is acquired. (However, in practice, true orthogonality is typically not possible.) This case is referred to as the *bit-by-bit code changing scheme* or *bit-nonhomogeneous code assignment.*

Near perfect capture can also be achieved by assigning distinct "orthogonal" codes to nodes. In this mode of operation, the preamble contains information on the spreading code used, allowing the receiver to program its matched filter accordingly. As long as transmitters are assigned orthogonal codes, perfect capture does not require bit-by-bit code changing. This mode of operation is referred to as the *transmitter-directed code assignment.*

Usually, some form of error-correction encoding is performed on the information to be transmitted prior to spread-spectrum coding, since true orthogonality of codes is not always guaranteed on a bit-wise basis and the background noise is not always negligible. Then, with the use of a decoder, the correction of bit or symbol errors can be done at the receiving end.

3.1.2 Channel Access Protocols

The conditions under which a node may access the channel are determined by a channel access protocol. In some protocols, these conditions are determined by various factors, including the state of the node wishing to transmit and the states of other nodes in the network. However, in other protocols, the rules governing the channel access policy reflect only local information acquired at the node, such as the states of neighboring nodes. Conse-

quently, these channel access protocols rely on the ability of a node to dynamically acquire local knowledge. In either case, the role of a channel access protocol is to efficiently control the use of the common radio channel. As described later, in a network, the channel signaling method, code-assignment scheme, and capture properties influence the choice of a channel access protocol.

For description purposes, we shall consider a packet radio network to be composed of N nodes spread out over some geographical area. The connectivity of the network is a known Boolean function specified by an NxN hearing matrix $\mathbf{H} = [h_{ij}]$, where $h_{ij} = 1$ if j can hear i, and 0 otherwise. Consequently, each nonzero entry h_{ij} in the hearing matrix corresponds to a bidirected radio link in the network between node i and node j. A link is denoted by $\tau\!<\!i,j\!>$, where node i is referred to as the *source* and node j is called the *destination.* A link is considered to be *active* whenever a transmission is taking place over that link. Similarly, a network can also be represented graphically by a directed graph where the nodes in the network are represented by the vertices and one-way connectivities are represented by directed edges.

Following the notation in Tobagi [14], we will assume that all edges in the graph representation of a packet radio network are bidirectional, and hence, that the hearing matrix H is symmetric. For any node i, let $\Gamma(i)$ denote the set of all nodes connected to it (including node i). Let $\Gamma^*(i) \triangleq \Gamma(i) - \{i\}$. The elements of $\Gamma^*(i)$ are called the neighbors of i. For a collection of nodes A, let $\Gamma(A) \triangleq \bigcup_{i\in A}\Gamma(i)$ and $\Gamma^2(A) \triangleq \Gamma(\Gamma(A))$. Given transmission link $\tau\!<\!i,j\!>$, a node k is said to be *hidden* with respect to the transmitting node i if k is not a neighbor of the source node i but is a neighbor of the destination node j, i.e., if $k \in \Gamma(j) - \Gamma(i)$.

For the protocols described herein, it is assumed that nodes attempt packet transmissions at random points of time defined by some point process. If a transmitted packet is not received correctly, or if a packet scheduled for transmission is inhibited by the operation of the protocol, then that packet is again considered for transmission at some future point in

time, determined by the scheduling point process.

There are several channel access protocols of particular interest.

(1) Pure ALOHA

In this protocol, when a node generates a packet, it transmits the packet immediately, unless it is already transmitting another packet. Pure ALOHA was first introduced by Abramson for the single-hop narrow-band ALOHA system, which uses separate channels for outbound and inbound traffic [15]. In Pure ALOHA, transmission has priority over reception. In narrow band systems or spread-spectrum systems in which the code assignments used allow an idle receiver to acquire any incoming packet, aborting the reception of a packet may be beneficial since the packet may be destined for another node.

(2) Disciplined ALOHA

In this protocol, a node transmits a generated packet immediately, unless it is busy transmitting or receiving another packet [14]. Consequently, this protocol is ideal for spread-spectrum systems in which receivers only acquire packets destined for them. For other networks, this scheme might lead to improved performance by some limited form of activity sensing. If a node acquires a packet not destined for it, it is highly likely that there is a neighboring node for which the packet is destined, and it may be advisable to inhibit transmission so as to increase the probability of correct reception of the earlier packet.

(3) Slotted ALOHA

In this protocol, the time axis is divided into equally sized slots [16, 17, 18, 19, 20]. A node with a packet scheduled for transmission in a particular slot initiates transmission at

the beginning of the slot. It is assumed that the entire packet transmission fits within the slot. Consequently, since the slot size is fixed, slotted ALOHA is best suited for fixed-size packets. In narrow band systems, the arrival of two or more packets in the same slot at a receiver results in the loss of all packets. Spread-spectrum systems with certain code-assignments encounter the same total loss effect, e.g., when all preambles use the same code, since then slot synchronization would always cause overlap among preambles in a given slot. Receiver-directed preamble code assignments would offer some improvement, but transmissions destined for the same receiver would still interfere with each other. Considering a slot size slightly larger than the packet transmissions time, and then randomizing the initiation of transmissions within a slot so as to achieve some degree of time-capture, offers still further improvement [21]. Under this modification, it is conceivable that the first packet to arrive at a receiver in a given slot will be acquired if later packets were delayed by sufficiently long periods of time.

(4) Carrier Sense Multiple Access (CSMA)

In this protocol, a node must be able to sense the presence of transmissions by its neighbors [22, 23]. In narrow band systems, this is simply accomplished by sensing carrier. If a node is not already transmitting and if no ongoing transmissions are sensed, then a scheduled packet will be transmitted by that node. In narrow band systems, in spite of carrier sensing, two factors remain that contribute to collisions. The first is the nonzero propagation delay between neighbors; given a transmission on link $\tau{<}i,j{>}$, all nodes in the set $\Gamma^*(i)$ are not inhibited from transmission until the transmission from node i has been sensed by them all. Hence, the propagation time from node i to its neighbors constitutes a *vulnerable period* for $\tau{<}i,j{>}$ as far as transmissions from $\Gamma^*(i) \bigcap \Gamma(j)$ are concerned. The second factor is *hidden nodes*; given that a transmission $\tau{<}i,j{>}$ has been initiated, nodes in $\Gamma(j) - \Gamma(i)$ cannot sense the presence of $\tau{<}i,j{>}$ and are thus never inhibited by that transmission. Consequently, the entire packet transmission time constitutes a vulnerable period for $\tau{<}i,j{>}$, as far as transmissions for hidden nodes are concerned. In spread-spectrum systems, the capability

of sensing the activity of neighboring transmitters depends on the mode of operation of the network [24]. For example, in systems employing space-and-bit-homogeneous codes, carrier sensing is done by simply observing the output of the matched filters corresponding to the desired waveform, while in systems using transmitter-directed bit-homogeneous or receiver-directed bit-homogeneous codes, activity sensing requires additional hardware. Since spread-spectrum already exhibits strong capture properties, it is not clear whether using CSMA in spread-spectrum systems improves overall network performance. Blocking transmissions may actually decrease network throughput in this case.

(5) Busy Tone Multiple Access (BTMA)

A busy tone on a separate channel, which is emitted by a node to indicate that it is currently busy receiving a packet, can alleviate the problem of collisions caused by hidden nodes [25, 7, 26]. The busy tone signal inhibits the receiver's neighbors from transmitting and thereby interfering with it. We will first consider its use in narrow band systems. In *Conservative BTMA (C-BTMA)*, a node emits a busy tone whenever it senses carrier due to the presence of a transmission. Consequently, a node may transmit only if no busy tone is sensed. Given that a transmission $\tau\langle i,j\rangle$ has been undertaken, a one-hop propagation delay constitutes a vulnerable period as far as transmissions from nodes in $\Gamma^*(i)\bigcap\Gamma(j)$ are concerned, and a two-hop propagation delay as far as transmissions from nodes in $\Gamma(j) - \Gamma(i)$ are concerned. In essence, all nodes within a two-hop radius around the transmitter are inhibited for a short time following the start of a transmission. In *Destination-based BTMA (D-BTMA)*, only the destinations of active links transmit the busy tone. In *Idealistic destination-based BTMA (ID-BTMA)*, the destination of every active link emits the busy tone, even if that node could not receive the packet destined for it. In *Receiving destination BTMA (RD-BTMA)*, the destination node emits a busy tone only if it is able to acquire the packet. Given that a transmission $\tau\langle i,j\rangle$ has been undertaken, the vulnerable period is equal to a two-hop propagation delay; after the vulnerable period, all nodes in the set $\Gamma^*(j)$ are inhibited from transmitting. RD-BTMA is somewhat idealistic, since a node

does not know immediately if a transmission is intended for it; rather, this information is available only after the packet header has been processed. In *Hybrid destination-based BTMA (HD-BTMA)*, a node first operates in C-BTMA until the header is processed, and then it operates in RD-BTMA. For spread-spectrum systems, receiving-destination BTMA is the most practical from an implementation standpoint. It is also referred to as *Locked-onto Destination BTMA (LD-BTMA)* [27]: a busy tone is emitted by the destination node whenever the link is active and the destination node is *locked onto* the packet. In this scheme, receiver-directed code assignment is assumed. Note that BTMA might have limitations for military purposes; a node emitting a busy tone signal would reveal its location to the enemy.

We remark that there exist a class of channel access protocols called *splitting algorithms*, wherein the main idea is to probabilistically split the terminals involved in a collision into transmitting and nontransmitting users with the process repeated in subsequent time units until all the terminals (involved in the collision) successfully transmit their packets. The tree algorithms developed by Capetenakis [28, 29], Hayes [30], and Tsybakov and Mikhailov [31] were the first of these algorithms. These algorithms were shown to achieve a much higher maximum throughput than ALOHA-type protocols, and, besides, were found to not suffer from the instability problem that plagues ALOHA-type protocols (see section 3.2.2). For excellent summaries of this research, along with further references, consult Gallager and Tsybakov [32, 33].

In a multihop packet radio network, the performance of channel access protocols is difficult to predict. The performance depends on the topology of the network and the resulting imposed traffic requirements. In narrowband systems with a fully-connected network, CSMA significantly outperforms ALOHA [23]; however, in a multihop network, the presence of hidden nodes can greatly degrade the performance of CSMA, and thus CSMA may be only slightly better than ALOHA. BTMA poses a slightly more complicated situation. A successful transmission in D-BTMA may have been inhibited in conservative BTMA. However, in D-BTMA, an unsuccessful transmission may occur, which blocks other potentially successful transmissions, while in C-BTMA, the former transmission would be inhibited by the

protocol, thus allowing the later, potentially successful transmissions to take place.

3.1.3 Link Scheduling

For networks in which the connectivity is established (e.g., using the LCA), it is necessary to determine a schedule for activating or enabling the links corresponding to these connections. A transmission schedule determines which set of links are allowed to transmit during each time interval. Again, it is desirable to realize this scheduling by a distributed algorithm. Moreover, it is desirable to have efficient schedules that do not have too many idle time slots during which no links are enabled. These schedules should also not only reflect fairness, but also be matched to the traffic flow patterns. An effective schedule prevents interference among transmissions from neighboring links.

An algorithm for link activation was developed by Baker, Ephremides, and Flynn, and was based explicitly on the use of the two TDMA transmission frames of the LCA [6], described earlier in section 2. The *Link Activation Algorithm* (LAA) consists of two phases: the allocation of slots and the resolution of scheduling conflicts. A detailed description is provided in Baker, Ephremides, and Flynn [6]. After the LAA was introduced, two events of interest happened. First, Hajek examined a general approach to the problem where the traffic matrix was taken into account and slots were allocated to minimize the number of secondary conflicts [34]. Second, it was observed by Hajek [34] and by Post, Sarachik, and Kershenbaum [35] that the problem of link activation scheduling has a strong resemblance to graph-theoretical problems, such as graph coloring.

(1) Biased-Greedy Algorithm

Post, Sarachik, and Kershenbaum [35] developed a heuristic, called the *"Biased-Greedy"* algorithm, to solve the link activation problem in a centralized fashion while using concepts from graph theory. The algorithm provides efficient communication by giving priority to

links with heavy traffic requirements. The essential idea of this algorithm is to activate as many nonconflicting links as possible in each time slot, thus maximizing channel utilization. (It is noteworthy that, in the context of tactical battlefield communications, maximizing the channel utilization may not be a feasible proposition, because of the danger of location identification of the mobile terminals.) The problem is equivalent to the graph theory problem of computing a *maximal matching* on the graph representing the network. Computing a matching on a graph consists of finding a set of edges of the graph such that no two edges are incident on the same node. A maximal matching is a matching where no edges can be added without violating the definition of a matching.

In the Biased-Greedy algorithm, for each time slot, a maximal matching is created by selecting the next unblocked link with the greatest remaining traffic. This selection process continues until there are no unblocked links remaining. The "greedy" aspect of the algorithm is evident in the selection of the "fattest" link, i.e., the link with the greatest amount of traffic. A bias is added to the traffic on each link in the network; the bias is equal to the traffic on the "fattest" link. The bias is subtracted from a link after it has been activated for the first time. Consequently, it is ensured that each link will be active at least once early in the schedule. Further details on the "Biased-Greedy" algorithm can be found in Post, Sarachik, and Kershenbaum [35]. In another paper, the same authors proposed a distributed version of the "Biased-Greedy" algorithm, called the *Distributed Evolutionary Algorithm* [36].

(2) Link Scheduling Using Cliques

Another approach, using the graph notion of *cliques*, has been taken by Silvester [37]. (A clique in an undirected graph $G = (V, E)$ is a subset $V' \subseteq V$ of vertices, where each pair of vertices is connected by an edge in E.) The basic idea of this algorithm was to first color the largest clique of traffic and then fill in the colors (slot schedules) for all remaining links. This

algorithm takes traffic requirements into account while providing conflict-free schedules.

(3) Transmission Scheduling Algorithm

For the ITF Network [1], it is not only important to form the schedules quickly with little communication overhead, but it is also important that any link and node failures during the execution of the scheduling algorithm do not leave any nodes unable to communicate. The Transmission Scheduling Algorithm (TSA) was also developed by Ephremides, Baker, and Wieselthier to provide scheduling of nodes for the ITF network [38]. TSA makes explicit use of the spread-spectrum signaling in the network; it is also distributed and addresses additional network requirements. It results in conflict-free transmission schedules that are produced quickly and with little communication overhead.

The TSA also uses the TDMA transmission frames similar to those used in the LCA. However, it alleviates some of the shortcomings of strictly scheduled, fixed TDMA protocols by creating flexible schedules. TSA allows for incorporating new nodes into the system as needed, adapts to varying traffic needs, and uses the cluster structure in LCA to improve on efficiency of channel utilization.

The TSA maintains two sets of parallel schedules, one network-wide fixed TDMA schedule and a set of separate transmission schedules, one for each cluster. The network-wide fixed schedule is like the one used for the two frames of transmission needed by the LCA. Each clusterhead schedules exactly one node at any given time slot in its own schedule. However, if desirable, the clusterhead may schedule several nodes during each time slot. In general, since there are fewer clusters than there are nodes, and since clusters tend to be spread out, the number of *secondary* conflicts will usually be small, i.e., other-user interference that results from signals that use codes that are quasi-orthogonal to that of the desired signal. The fixed network-wide schedule is used to ensure that each node is aware of at least some of the communication slots of every other node in the net, to allow for the addition of new nodes

into the network, and to enable the separate executions of the LCA in different frequency subbands at the corresponding reorganization periods.

Transmitter-based FH codes are used to avoid any *transmitter scheduling conflicts* that would arise when a node is scheduled to transmit on two schedules in the same time slot. Hence, most of the time a transmitter will use its own, unique FH code when transmitting. However, in cases when a new node is joining the net, the node may have to transmit using a code other than its own transmitter-based code.

The TSA shares the same transmission slots as the LCA and, hence, is said to "piggyback" onto the LCA. In the TSA, during its frame 2 transmission, each clusterhead announces the transmission schedule for the nodes of that cluster. Since the clusterheads may not be heard by all nodes, each node repeats, in its frame 2 transmission, the schedule announced by its own clusterhead. The clusterhead selection rule ensures that nodes that are not clusterheads hear from their own clusterheads before their frame 2 transmission. Consequently, every node becomes aware of at least two of the transmission schedules of all its neighbors, the network-wide fixed TDMA schedule, and the schedule announced by its own clusterhead for all the cluster members.

Although the addition of new nodes in a network operating under a TDMA protocol is difficult in a distributed environment, the TSA offers the flexibility to address this issue simply. (Alternately, nodes can employ a channel access protocol in place of TDMA in order to determine link schedules.) The network-wide fixed TDMA schedule is extended to include one or more contention slots. A node can freely transmit in these slots; however, it must use a separate, common code known to all potential network members. A node that wants to enter into the network must first monitor the channel to determine which nodes it can hear. At the first available opportunity, the new node may transmit a *network-entry* packet during one of the contention slots, using the special common code. At a minimum, this packet contains the ID number of the new node in addition to a list of all the nodes that the new node can hear. Consequently, nodes that receive the network-entry packet, and that are

also on the list, are bidirectionally connected to the new node. These nodes then save that packet until the next reorganization period, where they then broadcast that information in their scheduled slot during frame 1 of the LCA. If a clusterhead receives this information, it includes it in its new schedule. Thus the new node becomes part of the network without fully participating in the reorganization period.

(4) Network Evacuation

Recently, Tassiulas and Ephremides [39] considered the case of transmission schedules for network evacuation, in which nodes wish to deliver all their packets to a fixed, common destination. The authors assume that each node has a single transceiver. Thus, requiring that two links sharing a common node cannot be activated at the same time, ensures conflict-free transmissions. In such a scenario, the problems of route selection and link scheduling are coupled. However, the authors show that the joint optimization problem decomposes into a pure scheduling problem and pure optimization problem, both of which are studied in Hajek and Sasaki [40].

The authors use the idea of a *transmission set* in developing transmission schedules. A transmission set is a subset of links in the network that can be enabled simultaneously without conflicts, i.e., every two links that belong to the set do not share a common node. A schedule s of link activations is a sequence of pairs of a transmission set and the corresponding duration of its activation time. Formally, this is given by

$$s = \{(T_i, \tau_i), \quad i = 1, \cdots, N\}, \tag{1}$$

where N is the number of distinct activation epochs, T_i is a transmission set, and τ_i is the corresponding time epoch. The length of the schedule s is defined as

$$L(s) = \sum_{i=1}^{N} \tau_i. \tag{2}$$

Let S be the set of all schedules. Then the optimization problem can be stated as

$$\inf_{s \in S} L(s), \tag{3}$$

such that $q(L(s)) = 0$ when $q(0) = q_0$. ($q(t) \triangleq [q_1(t), \cdots, q_V(t)]$, where $q_i(t)$ is the amount of information that resides at node i at time t, and V is the number of nodes in the network. Thus, $q(0)$ is the initial amount of information residing at the nodes.) However, the previous dynamic optimization problem is of high complexity. The authors thus show that the problem can be reduced to two static (finite-dimensional) optimization problems of reduced complexity. Details on the reduction can be found in Tassiulas and Ephremides [39]. The resulting two optimization problems have been studied in Hajek and Sasaki [40], where algorithms for their solution are presented.

(5) Topology Transparent Link Scheduling

Chlamtac and Farago [41] addressed the problem of making transmission schedules immune to topology changes in a multihop packet radio network. They propose a *topology transparent* solution that incorporates random access protocols to scheduled link access. The protocol is independent of the detailed topology and depends only on *global* network parameters (number of nodes and maximum number of neighbors of a node). In deriving their solution, the authors use mathematical properties of finite (Galois) fields. The authors assert that the algorithm operates conflict-free under any rate of change, provided a maximum bound on the previous network parameters is observed in the network. For details on the algorithm, see Chlamtac and Fargo [41].

3.2 Modeling and Performance Evaluation

This section presents results obtained on the performance evaluation of packet radio networks. As the general analysis of these networks is rather difficult, the results surveyed here are with simplifying assumptions made on the network topology, channel access protocol,

channel signaling technique, and routing technique used.

The fundamental performance measures of a network are throughput, delay, and stability. The *throughput* measures the average rate of successful packet transmissions per unit time. The *delay* denotes the average time taken for a packet to traverse the network from source to destination. Various notions of network *stability* exist, but roughly, a network is stable if it does not reach a state where an excessively large number of packets are backlogged at the various nodes. For network performance evaluation, particular interest lies in the determination of the *capacity* (or maximum achievable throughput) and the tradeoff between throughput and delay. In the rest of this section, we survey the results obtained on both of these topics. For each topic, we treat the single-hop and the multihop cases separately.

3.2.1 Capacity Analysis

In this section, we consider analytical models appropriate for the determination of network capacity. Let the network input traffic requirement be denoted by the matrix $\Gamma = [\gamma_{jk}]$, where $\gamma_{jk}, j \neq k$ is the average number of packets per unit time offered at node j and finally destined for node k. Let $\gamma_{ii} = 0, \forall i$. Let γ denote the total user traffic, i.e.,

$$\gamma \triangleq \sum_{j=1}^{N} \sum_{k=1}^{N} \gamma_{jk}, \tag{4}$$

and define $\alpha_{jk} \triangleq \gamma_{jk}/\gamma$, where the matrix $[\alpha_{jk}]$ represents the traffic pattern. Then keeping the matrix fixed, the *network capacity* is defined to be the maximum value γ for which the network is stable.

The analysis of packet radio networks is greatly simplified by assuming that the *routing algorithm is fixed* (all packets from a given source to a given destination flow through the same set of nodes), all nodes have infinite buffers, and no flow nor link control protocols are present. While these assumptions do simplify matters, the capacity analysis of packet radio networks still remains complex due to the many operational characteristics, i.e., the

characteristics discussed in section 3.1. We discuss the special case of single-hop networks before proceeding to multihop packet radio networks. The models for the single-hop networks serve as precursors to multihop network models and thus offer tools for better understanding of the latter network.

(1) Single-hop: Capacity Analysis

Analysis of single-hop networks operating under a variety of channel access protocols has received much attention in the literature. While most analysis has focused on narrow-band systems with zero capture, some did address the case of spread-spectrum and time capture. Abramson [15] introduced and provided an analysis of pure ALOHA. Roberts [19, 20] followed with an introduction of slotted ALOHA, which was later analyzed by Abramson [16, 17], and Kleinrock and Lam [18, 42]. Kleinrock and Tobagi subsequently introduced and analyzed CSMA [22, 23] and BTMA [7]. Raychaudhuri analyzed slotted ALOHA with code-division [43]. Davis and Gronemeyer address spread-spectrum slotted ALOHA with capture due to time of arrival [21]. Musser and Daigle [44] derived the throughput of pure ALOHA with code-division. Pursley considered the throughput of frequency-hopped spread-spectrum communications [45]. Essentially, research in this area has given rise to two analytical models: an *infinite population* model and a *finite population model.*

The environment in the analysis of single-hop networks is assumed to consist of a population of nodes communicating with a *single* station. Radio connectivity need not exist among the nodes themselves for the ALOHA protocols. However, for CSMA it is assumed that all nodes are radio connected, and hence every terminal can sense the activity of every other node. This assumption is then relaxed allowing hidden nodes to be present.

We discuss the two analytical models briefly.

- *An Infinite-Population Model:* As suggested by the name, in this model the number

of users is assumed to be very large (infinite). Users generate packets at an aggregate rate of γ packets per second. Fixed-size packets with transmission time T seconds are assumed. If a time unit (also called a slot) is taken as T seconds, the packet generation rate becomes $S = \gamma T$ packets per slot. Assuming a large population, we see that the time taken to successfully transmit a packet is small compared to the time it takes it to generate a new packet. Consequently, no queueing of packets takes place, and all outstanding packets that are generated but not yet successfully transmitted belong to different nodes. As a result of packet collisions and blocking by the channel access protocol, the rate at which packets attempt transmission over the channel is larger than S, and it is denoted by G. In this model, it is also assumed that a packet that was blocked or unsuccessfully transmitted incurs a mean rescheduling delay X, which is very large compared to the packet transmission time. To simplify the analysis, if the process of new packet generation (due to all users) is Poisson with rate S, then the channel traffic process is traditionally taken as Poisson with rate G. Considering a channel traffic which is Poisson rate G simplifies the analysis of network capacity. The derivation of the corresponding rate of successful packets S leads to $S = GP_s$, where P_s is the probability that an arbitrary scheduled packet is successful. P_s varies with the channel access protocol and capture properties used. Since the packet size has been assumed to be of fixed size, S also represents the throughput. In systems employing pure ALOHA with zero capture, the throughput is given by $S = Ge^{-2G}$, and for slotted ALOHA $S = Ge^{-G}$; for nonpersistent CSMA the throughput is given by $S = (Ge^{-aG})/[G(1+2a) + e^{-aG}]$, where a is the ratio of propagation time τ to packet transmission time T. Pessimistically, τ is assumed to be the same for all pairs of users. Similar expressions for throughput can be derived for other access schemes and other capture assumptions. The network capacity C is obtained by simply maximizing S with respect to G, e.g., $C = 0.18, 0.36, 0.85$ for pure ALOHA, slotted ALOHA, and CSMA ($a = .01$), respectively.

- *A Finite-Population Model:* In his analysis of slotted ALOHA, Abramson also considered a finite-population model [16, 17, 46]. The model consists of N nodes numbered

$1, 2, ..., N$. Node i ($i = 1, ..., N$) follows a Bernoulli process with rate G_i to determine the slots during which to transmit packets. The rate of channel traffic due to node i is then G_i, assuming that at each such slot node i does actually have a packet to transmit. The total channel traffic is

$$G = \sum_{i=1}^{N} G_i. \tag{5}$$

Let S_i denote the probability that node i transmits a packet and is successful. The throughput for node i is also represented by S_i. The total throughput is given by

$$S = \sum_{i=1}^{N} S_i. \tag{6}$$

The assumption that *nodes always have packets to transmit* leads to the following set of expressions.

$$S_i = G_i \prod_{j=1, j \neq i}^{N} (1 - G_j), \quad i = 1, \ldots, N. \tag{7}$$

This set of equations is used to determine the boundary of the stability region for $\{S_i\}_{i=1}^{N}$ by computing the Jacobian $J = J(S_1, S_2, \cdots, S_N; G_1, G_2, \cdots, G_N)$, and then setting it equal to zero. By doing so, this leads to the condition $\sum_{i=1}^{N} G_i = 1$. For a given traffic pattern $\{\alpha_i\}_{i=1}^{N} = \{S_i/S\}_{i=1}^{N}$, the network capacity is then given by the point on the surface which corresponds to its intersection with the line

$$S_1/\alpha_1 = S_2/\alpha_2 = \cdots = S_N/\alpha_N. \tag{8}$$

Let $\{C_i\}_{i=1}^{N}$ denote that intersection point. Then the network capacity C is given by

$$C = \sum_{i=1}^{N} C_i. \tag{9}$$

Note that $C = \max_{\{G_i\}_{i=1}^{N}}(S)$ such that $S_i = \alpha_i S, \forall i$; C is achieved by a *unique* set of transmission rates $\{G_i^*\}_{i=1}^{N}$.

- *The Hidden Terminal Problem in CSMA:* As mentioned in section 3.1.2, CSMA suffers performance degradation in the presence of hidden terminals. Tobagi and Kleinrock

addressed this problem for single-hop networks [7]. They consider a model consisting of a large number of terminals communicating with a single station, where packet size is fixed. While all nodes are in LOS and within range of the station, they are not with respect to each other. All assumptions introduced for the infinite population model also hold true. The population is partitioned into say N groups as determined by the hearing matrix describing connectivity for the environment. All nodes within a group hear each other and hear the same subset of nodes in the rest of the population. Each group is assumed to consist of a large number of nodes that collectively form an independent Poisson source with mean rate S_i packet per unit time. Then given a traffic pattern

$$\{\alpha_i\}_{i=1}^N \triangleq \{S_i/S\}_{i=1}^N, \tag{10}$$

where

$$S = \sum_{i=1}^N S_i, \tag{11}$$

the problem is to find $\{C_i\}_{i=1}^N$ such that

$$C \triangleq \sum_{i=1}^N C_i = \max S \tag{12}$$

and $C_i = \alpha_i C$. Letting G_i denote the rate of channel traffic offered by group i, it can be shown that [7]

$$S_i = G_i f_i(G_1, G_2, \ldots, G_N), \ i = 1, \ldots, N. \tag{13}$$

These equations are similar to those obtained with the finite-population model previously mentioned; the difference is the complexity of the equations, which requires numerical procedures for determining the network capacity.

(2) Multihop: Capacity Analysis

Gitman [47] derived the network capacity for a two-hop centralized multihop network consisting of user terminals communicating with a single station via repeaters located around

the station, and operating under slotted ALOHA. The analytical model used is a combination of the infinite-population model representing the terminals, and Abramson's finite population model representing the repeaters. Tobagi considered the same topology and derived the network capacity as well as the throughput-delay characteristics for both CSMA and slotted ALOHA. He discussed their dependence on such key parameters as transmission protocols, repeater connectivity, and repeater storage capacity. The capacity of one-way tandem slotted ALOHA networks was analyzed by Yemini [48].

In this section, we consider the analysis of network capacity for systems with a general topology operating under any possible combination of channel access protocol and capture mode. We describe the different models that have been proposed and discuss the major results obtained for each. We then show how Tobagi [14] extended the model for slotted ALOHA introduced by Abramson to study networks with general topologies.

Boorstyn and Kershenbaum [49] addressed the use of continuous-time processes to study networks. They derived a Markovian model for the analysis of a network with general but symmetric hearing matrix, zero-propagation delay, operating under CSMA, with the assumption that the first packet to arrive at a receiver after the channel has been idle is captured perfectly, and all other packets are lost. The authors observed that under the previous conditions, a sufficient state description for the network is the *set of transmitting nodes.* Analysis of network capacity led to a steady-state distribution with a product form and simple throughput equations, thus allowing for the design of efficient algorithms for the analysis of large networks [50]. Tobagi and Brazio considered the same model for ALOHA with zero and perfect capture, and C-BTMA with perfect capture [51]. C-BTMA with perfect capture was also addressed by W. C. N. Chen [52]. Tobagi and Brazio made the important observation that not all protocols could be modeled by simply tracking the set of transmitting nodes, nor could they all lead to a product form solution. They later took a different approach to the model by considering the state description to consist of the set of transmitting nodes along with their respective intended receivers, which constitutes the set of *active links* [53]. Networks with nonsymmetric hearing matrices and other access schemes

could easily be accommodated by this extended model. Appropriate conditions on network topology, traffic requirements, and access protocols were provided that enabled the analysis to lead to a steady-state distribution with a product form. With the results obtained, the network capacity for narrow-band systems could be determined for various topologies under CSMA, pure ALOHA, C-BTMA, and ID-BTMA.

These models all accommodate systems in which the capture of a packet at its intended receiver, and the decision of a node to transmit, depend only on the set of active links just prior to the transmission. Since spread-spectrum systems operate differently, these model are not well suited for them. For spread-spectrum systems, it is necessary to know the state of the receivers (locked onto a packet or idle) in addition to the set of active links. Brazio and Tobagi modified the state description to include the state of the receivers [24]. They specifically addressed access protocols (pure ALOHA, CSMA, and BTMA) for which the decision whether to transmit or not can be considered a function of only the set of active links, independent of the state of the receivers. The analysis for disciplined ALOHA and locked-onto destination BTMA has also been done [27]. M. S. Chen and Boorstyn focused on the disciplined ALOHA, receiver-directed CDMA protocol [54, 55]. They analyzed networks of general topology with several hundred nodes. A noise model is introduced and analyzed by setting a threshold on the number of transmitting neighbors that would cause packet loss. A more detailed model of a node and link was considered by Sen [56], which enabled better approximations. Yemini took a completely different approach to modeling packet radio networks by using techniques of statistical mechanics [57]. (For more details, see Kleinrock and Silvester [58].)

The following are brief descriptions of network models used for the analysis of the capacity of networks with a general topology operating under different combinations of channel access protocol and capture mode:

- *Network Abstraction and General Model [14]:* Given a static routing pattern, the

throughput requirement for each link $\tau\!<\!i,j\!>$ is denoted by S_{ij}. S_{ij} can be computed as a function of the end-to-end traffic requirements Γ. For some links, the required throughput may be zero. These links are referred to as *unused links*, all other links being *used links.* Each node in the packet radio network has one transmitter, but in general more than one outgoing link. Each outgoing link at a node has a separate queue for the packets that are to be transmitted on it; the transmitter is shared by all queues at that node. Transmission requests for the various queues at a node are scheduled according to random processes in order to avoid repeated interference between transmissions in the network. A scheduled transmission may or may not take place depending on the status of the transmitter at the source node (busy or idle), the channel access protocol being used, the priority structure among the different queues at the source node, and the current activity on the network. If the transmission is inhibited or if the transmission is unsuccessful, then the packet is reconsidered at the next scheduled transmission. When the transmission of a packet is successful, it is removed from the queue.

The assumptions are that neither preemption nor priority functions are in effect at the nodes. In addition, infinite buffer space for each link, zero propagation delay between neighboring nodes, and instantaneous and perfect acknowledgments (providing immediate feedback on the success or failure of each transmission) are assumed. It is assumed, for the purposes of network capacity, that at each scheduling point of the point process there is a packet in the queue.

- *Slotted ALOHA [14]:* In modeling slotted ALOHA, it is assumed that the scheduling process which governs transmissions over link $\tau\!<\!i,j\!>$ is Bernouilli with parameter G_{ij} and is independent of all other such processes in the network. Let $G_i = \sum_j G_{ij}$ and $G_i \leq 1$ since each node has only one transmitter. The memoryless and independence properties of the Bernouilli process, and the assumption that no queue is ever empty, allow the network's behavior to be studied by examining one arbitrary slot. The throughput equations can be written for any slot, taking into account the specific

network topology. The throughput for systems of zero capture is given by

$$S_{ij} = G_{ij} \prod_{k=1, h_{jk}=1}^{N} (1 - G_k). \tag{14}$$

For a given traffic pattern, the network capacity can be determined by an iterative numerical procedure. The same analytic procedure can be used for slotted ALOHA in spread-spectrum systems with code-division or time-capture. Gitman provided an analysis of two-hop centralized networks [47], and Silvester and Kleinrock applied this method to study the capacity of slotted ALOHA networks with regular structure [59].

Since the models for slotted and unslotted ALOHA do not follow the evolution of packets as they are forwarded from source to destination, they do not accurately represent the multihop operation of a network. The models, however, attempt to represent the interactions that exist among nodes and their respective effects on throughput.

- *Transmitter Activity Model for Unslotted Networks:*

  (a) CSMA with perfect capture of first packet following idle channel in networks with symmetric hearing matrix [49]: Boorstyn and Kershenbaum model the scheduling point process for each used link $<i,j>$ as Poisson with mean λ_{ij}, independent of all other such processes in the network. For messages transmitted by node i, the message lengths are considered to be exponentially distributed with mean transmission time $1/\mu_i$. Each node has a large number of messages waiting to be transmitted, and at each scheduling point a different message is considered. Since different nodes have different mean message transmission times, the nodes may be transmitting at different data rates; the length of all messages in bits is considered to be drawn from the same distribution.

  For a network with zero propagation delay, given CSMA and the previously mentioned capture assumption, a scheduling point for link $<i,j>$ results in a successful transmission if and only if all nodes in the set $\Gamma(i,j)$ are idle at the scheduling point. Each scheduling point is random since the scheduling process is Poisson. The average time of a successful transmission is $1/\mu_i$. The throughput S_{ij} is given by

$$S_{ij} = \frac{\lambda_{ij}}{\mu_i} \Pr(\Gamma(i,j) \text{ idle}) \tag{15}$$

Since the hearing matrix is symmetric, it is sufficient to consider the process $X(t), t \geq 0$, where $X(t)$ is the set of nodes busy transmitting at time t, to compute $\Pr(\Gamma(i,j)$ idle). A detailed description of the derivation of network capacity can be found in Tobagi [14].

(b) Pure ALOHA and C-BTMA in networks with symmetric hearing matrix: The state description required for the analysis of ALOHA and C-BTMA in symmetric topologies was shown to be the set of nodes busy transmitting [51]. In both the perfect capture and zero-capture cases, a necessary condition for a scheduling point for link $<i,j>$ to result in a successful transmission is that $\Gamma(j)$ be idle at that time. The average length of a successful transmission is no longer $1/\mu_i$. The success or failure in the reception of a packet is dependent on the state of the network at the beginning of reception, as well as any events that may occur during its reception. Further details are provided in [14].

- *Link Activity Model [53]:* Brazio and Tobagi introduced the link activity model to address networks with nonsymmetric hearing matrices and such access schemes as ID-BTMA. The attention is still on access protocols in which the decision whether to transmit can only be based on the state of the transmitters, and not on the receivers. For the access protocols that are considered, when given the current set of active links in the network, a protocol is a set of rules that will determine whether or not a given inactive link can become active. All used links are numbered $1, 2, ..., L$ and let $LL = \{1, 2, ..., L\}$. The point process for link $i, i \in LL$, is considered to be an independent Poisson process with rate $\lambda_i, \lambda_i > 0$. The transmission time of the messages transmitted over link i is assumed to be from an exponential distribution with mean $1/\mu_i, \mu_i > 0$. The transmission times are to be redrawn independently from this distribution each time the message is transmitted. Let $X(t)$ denote the set of all active links at time t; X(t) is a continuous-time Markov chain. See Tobagi [14] for further details.

- *Models for Spread-Spectrum Systems:* Thus far the models mentioned focus on access protocols where the outcomes of transmissions are independent of the receiver's state

at each node. These models are valid for some narrow-band systems; however, for the analysis of other narrow-band systems (e.g., BTMA) and spread-spectrum systems, the operation of the receiver must be incorporated. At any given time, each node may be in one of three basic states: idle, transmitting, or receiving (locked onto a packet).

A general Markovian model [24, 27]: For a node to receive a packet correctly, the node must be idle, it must process the preamble successfully, and it must complete the reception of the packet free of error. If a node is idle, then the probability that it acquires the incoming packet depends on many factors, including the set of links which are active at the start of the preamble, and the evolution of the system during the reception of the preamble. While an accurate model of most of these factors is possible, the complexity arises from having to track the evolution of the system during the reception of the preamble. This would lead to non-Markovian models. Ephremides first considered models of probabilistic capture [60, 61]. Brazio and Tobagi [24] later introduced a model of the operation of receivers that maintains the tractable Markovian nature of the model. Given the set of links D which are active just before the start of transmission of some link j, the model assumes that if the receiver at node n is idle, it successfully acquires $j's$ transmission with probability $P_n(D;j)$, independently from trial to trial. By appropriately selecting $P_n(D;j)$, the preamble capture behavior of both space-homogeneous and receiver-directed preamble codes can be properly modeled. If a preamble is not successfully received, the receiver will remain idle, waiting to acquire a new packet. If the preamble is correctly received, then the receiver remains synchronized to the data portion of that packet until the end of transmission. The capture mode in effect and the activity of the transmitters in the network during the packet reception time thus affect the outcome of the transmission. Extensive details are provided in Tobagi [14].

3.2.2 Throughput-Delay Tradeoffs

For capacity analysis, if we assume a node has a packet for transmission at each scheduling point, then it is not necessary to include information regarding the number of packets in queue at each link. At capacity, the packet delay is infinite. However, below capacity, queue lengths are not infinite and must be included in the state description. Consequently, analysis becomes complex since the state space grows substantially. The need to keep track of the evolution of packets through the network poses another problem in the delay analysis for multihop packet radio networks. Again, additional information must be included in the state description. In literature thus far, two approaches are taken: (1) exact analysis of specific systems, generally small in size or simple in their topological structure, and (2) approximate analysis requiring a reduced state-space description of more general and larger topologies.

Much of the literature in this area has focused on single-hop networks and their throughput-delay analysis. These studies have aided in the understanding of the behavior of multiaccess channels and in modeling multihop networks. We first address the work done on single-hop systems and then proceed to multihop networks.

(1) Single-hop: Throughput-Delay Tradeoffs

It is assumed that all nodes are *identical* and that each has a *single packet buffer*. A node is either in an *idle* state when its buffer is empty, or in a *backlogged* state when its buffer is nonempty. While a backlogged node does not generate new packets, it follows the channel-access protocol in attempting to transmit its packet. After successfully transmitting, a node becomes idle, and thus generates a new packet after a *random* thinking time. With the assumption that the scheduling process and distribution of thinking time at each node is memoryless, a complete description of the state of the network is given by just the number of backlogged users. The process representing the system state is then Markovian. Kleinrock and Lam provide an analysis of slotted ALOHA [42], and later, Tobagi and Kleinrock analyze

CSMA [62]. Tobagi derived the distribution of packet delay and interdeparture times for both slotted ALOHA and CSMA by using the same model [63].

The previous analyses provide a definition and understanding of the stability of systems using multiple-access [64]. It was shown that depending on the system parameters (e.g., number of nodes, rescheduling delay) the system exhibits either a *monostable* or a *bistable* behavior. In a monostable system, there is a single equilibrium point, and for the bistable system, there are two equilibrium points. (An equilibrium point is a network state for which the mean rate of new packet generation is equal to the mean throughput rate.)

Tobagi and Kleinrock address the issue of single-hop packet radio networks with larger numbers of buffers per node [65]. They discuss a system in which two nodes with infinite buffers each communicate with a station over a slotted ALOHA channel. Kleinrock and Yemini examined the case of two interfering queues [66]; later, Sidi and Segall also studied the same case in a series of papers [67, 68, 69]. The solution of two nodes with infinite buffers was obtained by Nain [70] following the work by Fayolle and Iasnogorodsky [71]. Saadawi and Ephremides [72] derived an approximate solution for the delay in a slotted ALOHA, single-hop system with a finite number of identical nodes.

(2) Multihop: Throughput-Delay Tradeoffs

In the literature, the focus on throughput-delay for multihop packet radio networks has mainly been for slotted ALOHA with zero capture. For slotted ALOHA, the state of all nodes in a given slot determines the activity and outcome of the next slot. However, for unslotted systems, there are no designated times as slot boundaries; and hence, accounting for packet length, propagation times, etc., is more difficult. We will first discuss those studies which provide exact analysis of specific networks, and later, we will address approximate methods for more general networks.

(1) *Exact Analysis:* The first analysis of throughput-delay performance in multihop packet radio networks focused on a centralized two-hop system [73, 74, 75, 76]. Terminals communicate with a central station via repeaters with finite buffers located around the station. Hence, the first hop is from terminals to the repeaters, and the second hop is from the repeater to the central station. Slotted ALOHA and CSMA are addressed, considering only the inbound traffic. Specifically, the studies have focused on the effects on performance of the number of repeaters, the connectivity among the repeaters, the channel access protocol being used, and the number of buffers each repeater possesses. A significant result is that, assuming zero-processing times at the nodes and instantaneous acknowledgments, packet radio networks are *channel bound* rather than storage bound. A slight improvement is gained by increasing the buffer size at the repeaters from 1 to 2, but no substantial improvement is gained thereafter. Fuduka and Muramatsu later analyzed the same two-hop network addressing similar issues using the EPA techniques [77].

Studies focusing on more general topologies with exact analysis of specific instances have also been done [78, 79]. Since the models used give rise to a large number of states, they are applicable for small networks and, thus, are used to study some specific protocol features in small networks. Two arbitrary networks with 8 and 12 nodes, operating under slotted ALOHA, have been considered by Takagi and Kleinrock [79]. Roy and Saadawi [78] derived an exact analysis of throughput and delay in a multihop packet radio network employing a form of CSMA with busy tone and collision detection. A scheduled packet is transmitted by a node if it is idle and it does not detect carrier or a busy tone generated by a neighbor.

(2) *Approximate Analysis:* Approximate analyses assume that packets are independently generated at each node for transmission to a neighbor. Consequently, the amount of traffic generated is a function of the topology, routing protocol, and end-to-end traffic requirements. In the model used for approximate analysis, a representation of the neighborhood of a node is developed, which is characterized by a number of parameters representing average behavior. Leiner provided one of the first approximations for

analysis of throughput delay in multihop networks [80]. Later, Lee and Silvester [81, 82] used a more detailed model of the behavior of a node and developed an approximate analysis. Sen [56] considered disciplined ALOHA receiver-directed CDMA and used detailed models for nodes and links to provide an approximate analysis.

4. Routing

This section focuses on techniques that are commonly used to route packets through packet radio networks. The problem of packet routing resides within the *network* layer of the seven-layer OSI network architecture model.

Given the network organization and the protocols for media access, the problem of routing a packet reduces to finding a "best" sequence of links to be traversed by a message on its way to its final destination. In general, the problem of routing packets is of a multihop nature since packets may need to pass through intermediate (relay) nodes before reaching their destination. A routing algorithm must then perform two main functions: (1) selection of routes for various origin-destination pairs and (2) the delivery of messages to their correct destination once the routes are selected. Noteworthy is the emerging trend in the literature to consider routing algorithms in which network connectivities are determined as part of the routing process.

While every routing algorithm will make routing decisions, the times at which these decisions are made depend on whether the network uses *datagrams* or *virtual circuits*. In a datagram network, a routing decision is made for each individual packet; consequently, two packets of the same source-destination pair may traverse different paths. However, in a virtual circuit network, a routing decision is made for each source-destination pair, i.e., each time a virtual circuit is set up. Thus, all packets of the virtual circuit use the same routing path to send packets until either the virtual circuit is terminated or rerouted.

Routing in a network can be a complex issue. The complexity is due to a number of factors:

(1) Routing requires coordination between all the nodes of the network.

(2) The routing algorithm must adapt to node or link failures by redirecting messages and updating necessary databases maintained by the system.

(3) The routing algorithm may need to modify its routes to accommodate changes in traffic conditions; e.g., when some portions of the network become congested, the packets are routed through nodes elsewhere in the network.

The performance of a routing algorithm is primarily measured by the *throughput* and the *average packet delay.* When the traffic load offered by the network is relatively low, it will be completely accepted into the network and the throughput is defined as

$$\text{Throughput} = \text{Offered load.} \tag{16}$$

However, when the traffic load offered is excessive, a portion will be rejected and the throughput becomes

$$\text{Throughput} = \text{Offered load} - \text{Rejected load.} \tag{17}$$

The traffic that is accepted by the network will encounter an average delay per packet that is dependent on the routes chosen by the routing algorithm. Since flow control protocols find a balance between throughput and delay, the throughput of the routing algorithm will also be affected.

One way to classify routing algorithms is to divide them into *centralized* and *decentralized* algorithms. In a centralized algorithm, the routing decisions are made at a central node, while in a distributed algorithm, the task of route selection is shared among all the network nodes with information exchanged between them as necessary.

Another classification of routing algorithms is to categorize them as *static* or as *adaptive* (*dynamic*). In static routing algorithms, the routing paths used by each origin-destination pair is fixed regardless of changes in traffic conditions; routes are only altered as warranted by link or node failures. However, in adaptive routing algorithms, the routing paths used between origins-destination pairs can change occasionally in response to congestion.

Finally, routing algorithms can also be classified as *distance vector algorithms* or *link-state algorithms.* In a distance vector algorithm, each node has only local knowledge and shortest paths are computed using a distributed-type algorithm, such as the distributed Bellman-Ford algorithm [83]. In a link-state algorithm, global knowledge of the entire network (characteristics of all nodes and links) is available to all nodes, and a centralized algorithm (e.g., Dijkstra's algorithm [83]) is used locally at each node to compute the shortest paths to other nodes. A variation of link-state algorithms is *link-vector* algorithms that employ selective spreading of link-state information.

The remainder of this section is dedicated to describing various routing algorithms. We first briefly address two commonly used approaches for static routing. (Extensive treatment of other static routing algorithms and network routing in general can be found in [83].) We then provide a comprehensive survey of recently suggested adaptive routing approaches found in the literature. Where possible, we will compare and contrast the different algorithms.

4.1 Static Routing

Static routing is mostly used in simple networks or networks where efficiency is not critical. Since a static routing algorithm does not respond to traffic variations, it does not achieve a high throughput for a broad variety of traffic input patterns.

An important approach to static routing is *shortest path routing.* In a shortest path routing algorithm, a *length* is assigned to every link in the network, and the objective is to find a

path between two given nodes that have a minimum total length. When the length of each link reflects the congestion of the link, the shortest path route is then the *least congested* path between the two nodes. Two standard algorithms for the shortest path problem are described next. In these algorithms, the shortest paths from a given source node to all other nodes are found.

4.1.1 Bellman-Ford Algorithm

Consider a graph where the link lengths can be positive or negative, but no cycles of negative length are allowed. Let node 1 be the "source" node; then the problem reduces to finding the shortest paths from node 1 to every other node in the graph. Let d_{ij} denote the length of the link between node i and node j, and let $d_{ij} = \infty$ if (i, j) is not an edge in the graph. The main idea in the Bellman-Ford algorithm is to first find the shortest path lengths consisting of at most one link, then to find the shortest path lengths with at most two links, and so forth. The shortest path with at most h links will be referred to as the shortest $(\leq h)$ path.

Let $D_i^{(h)}$ be the shortest $(\leq h)$ path length from node 1 to node i. (Then $D_1^{(h)} = 0$ for all h.) The algorithm can then be summarized as follows:

For $h = 0$,

$$D_i^{(0)} = \infty, \qquad \forall i \neq 1. \tag{18}$$

For each successive $h \geq 0$,

$$D_i^{(h+1)} = \min_j \, [D_j^{(h)} + d_{ji}], \qquad \forall i \neq 1. \tag{19}$$

A resulting shortest path can contain at most $N-1$ links (where N is the number of nodes). In the worst case, the algorithm must be iterated $N-1$ times, each iteration for $N-1$ nodes,

and, for each node, the minimization must be taken over $N-1$ alternatives. Consequently, the running time is $O(N^3)$, where $\frac{O(N^3)}{N^3} \longrightarrow c$ (constant) as $N \longrightarrow \infty$. Further details can be found in Bertsekas and Gallager [83, p. 318].

4.1.2 Dijkstra's Algorithm

In this algorithm, all link lengths are assumed to be positive. The worst-case computational requirements for this algorithm are significantly lower than those of the Bellman-Ford algorithm. The main idea of this algorithm is to find the shortest paths in order of *increasing* path length. Let node 1 be the source node. Then the shortest of all the shortest paths from node 1 is the single-link path to the closest neighbor of node 1 (any multiple-link path must be longer than the first link length by virtue of the positive link length assumption). The *next* shortest of all the shortest paths is either the single-link path to the *next* closest neighbor of 1 or the shortest two-link path through the previously chosen node, and so forth. Formally, the algorithm can be described as follows:

Let P be the set of *labeled* nodes. At each step of the algorithm, the node added to P will be the closest neighbor of node 1 out of those nodes that are not yet in P.
For each node i, let D_i be an estimate of the shortest path length from node 1 to node i.
Let d_{ij} denote the length of the link between node i and node j.
Initially, $P = \{1\}$, $D_1 = 0$, and $D_j = d_{1j}$ for $j \neq 1$.
Step 1: Find the next closest node, i.e., find $i \notin P$ such that

$$D_i = \min_{j \notin P} D_j. \tag{20}$$

Set $P := P \cup \{i\}$. If P contains all nodes, then the algorithm is complete.
Step 2: Updating of path lengths, i.e., $\forall j \notin P$ set

$$D_j := \min[D_j, D_i + d_{ij}]. \tag{21}$$

Go to Step 1.
Each step in this algorithm requires a number of computations proportional to N, and the

steps are iterated $N-1$ times. Consequently, the worst-case computation is $O(N^2)$. Further details can be found in [83, p. 322]

4.1.3 Disjoint Shortest Path Routing

A different approach to the shortest path routing problem is to find paths that are not only short, but also *disjoint*. Two paths between a source and destination are considered disjoint if the paths do not share any nodes (and hence links), other than the source node and destination node. Torrieri [84] presented a routing algorithm to find optimal sets of short disjoint paths between any source and destination pair. Torrieri asserts that searching for two or more disjoint paths between a source node and a destination node has the following advantages: (1) network reliability and survivability are reinforced, (2) node or link failures do not have to be isolated immediately, (3) multiple-path routing usually provides the optimal solution when network-wide time delay is to be minimized [85], and (4) there is no potential looping problem, i.e., when a path fails and a new path is assigned.

4.1.4 Deeper Issues in Shortest Path Routing

In network routing, there are deeper issues than simply finding shortest paths, since the shortest path may not be the most desirable. The essential goal is to minimize the *delay* experienced in going from a source to a destination; the delay associated with each link is generally a function of the amount of traffic carried by the link; if a link is heavily used, it becomes congested and it takes longer for a packet to traverse the link. The traffic carried by a link is referred to as *link flow* and is measured in units of packets per second. Given a desired flow level from source to destination, the problem is to distribute the flow among all possible paths from source to destination such that the total delay is minimized. Ephremides and Verdu provide a detailed formulation of this continuous optimization problem and also offer further insights into the general problem of packet routing [86].

4.2 Adaptive Routing

Adaptive routing algorithms respond to the dynamic nature of a network, while forming routing paths. In many networks, e.g., mobile networks, not only are the traffic conditions subject to change, but so are the network topological connectivities and individual link qualities.

4.2.1 Flooding

When nodes move often or when links fail intermittently because of jamming, there may not be enough time to accumulate global connectivity information to determine routes. In extreme cases of mobility when topological changes are too frequent, it is almost mandatory to impose *flooding*, i.e., the rebroadcasting of a message throughout the network. While flooding has some adverse effects, such as increased congestion, it is the only means of ensuring the delivery of information. The intermediate case in which the network does not change frequently enough to warrant flooding, and at the same time does not stay reasonably static long enough to make the "shortest route" method acceptable, is the most interesting and difficult scenario. An important consideration in networks with a "mid-frequent" rate of topological change is that the routing algorithm should not have excessive overhead; the algorithm should be able to react to topological changes and establish routes before the routes become obsolete with another topological change.

4.2.2 "Search and Discover" Routing

To address the intermediate scenario, a version of a highly adaptive "search and discover" approach was formulated in Bates [87]. In this approach, a node would flood a high-priority short query message through the network, thereby discovering a route that would lead to the destination node. Once the first link of that route was determined via a positive acknowl-

edgment mechanism, it would be used until a negative mechanism was received, indicating either that this route is no longer available or that it is heavily congested.

4.2.3 Hierarchical Routing

Another approach involves an idea similar to that of hierarchical routing as used in Packet Radio Network (PRNET) and Southern Universities Regional Association Network (SURAN) [6]. This approach uses the natural hierarchy provided by the linked cluster architecture (see section 2). This architecture supports routing by:

(1) identifying clusterheads for use in the regional or net-wide broadcasts of messages, and

(2) defining a backbone network over which inter-cluster communication can be concentrated.

By virtue of the architecture, all nodes in a cluster are within one hop from a clusterhead. Consequently, it is sufficient for every clusterhead to broadcast a message to achieve net-wide coverage.

In general, distributed routing schemes [88, 89, 90, 91, 92] can generally be characterized by four primary components: (1) the metric used to assign weights to individual links, (2) the method used to propagate the assigned link weights throughout the network, (3) the algorithm used to determine the *best* paths based on these weights, and (4) the procedures for storing and updating the necessary routing information in the individual nodes.

4.2.4 Tier Routing

The *tier routing* scheme, which was developed for the DARPA packet radio and used in the SURAN protocol suite [93, 88, 92], is a distributed scheme which selects routes that minimize the distance measured in number of hops. For the metric in tier routing, each good link is assigned weight 1 and each bad link is assigned weight ∞. A Bellman-Ford type algorithm is then used to determine the best routes [93, 88].

4.2.5 Distributed Bellman-Ford

A variation of the Bellman-Ford algorithm requires nominal information to be stored at the nodes and computes distances between nodes by means of a *distributed* version of the Bellman-Ford algorithm. Hence, it is called the distributed Bellman-Ford (DBF) algorithm. In this algorithm, a node only requires knowledge of the length of its outgoing links and the identity of every node in the network. A detailed description of DBF is given in Bertsekas and Gallager [83]. The brief description which follows is from Awerbuch, Bar-Noy, and Gopal [94]. Let $DBF(s,t)$ be the distributed Bellman-Ford algorithm that finds the shortest path in the network between node s and node t. In the algorithm, each node y maintains a *label* $a(y)$ of the current known shortest distance from node s to node y, and a variable *parent*(y), which contains the identity of the previous node on the current known shortest path between node s and node y. At the initial step $a(s) = 0, a(y) = \infty$, and *parent*(y) is undefined for all $y \neq s$. At the termination of the algorithm, $a(y)$ is the length of the shortest path from node s to node y, and $a(t)$, the desired value, is the length of the shortest path from node s to node t. The DBF algorithm consists of two basic rules: the *adopting rule* and the *sending rule.* While the adopting rule is used to update the current label according to a message from a neighboring node, the sending rule determines the specific values to propagate to the neighbors. Hence, the sending rule is employed whenever a node adopts a new label and thus must propagate this information to its neighbors.

- *The Adopting Rule*: Suppose node x, with label $a(x)$, receives $a'(x)$ from node z. If $a'(x) < a(x)$, then node x adopts $a'(x)$ and sets the value of *parent*(x) to z.

- *The Sending Rule*: Let $a(x)$ be a new label adopted by node x and let node y be a neighbor of node x other than *parent*(x). Then node x sends $a(x) + l(x, y)$ to node y, where $l(x, y)$ is the length of the link between node x and node y.

Under some scenarios, the distributed Bellman-Ford algorithm has exponential message complexity.

4.2.6 Gafni and Bertsekas Algorithm

Gafni and Bertsekas [95] examine a network with a central station which is subject to frequent topological changes. In such a network, the central station collects information regarding global network connectivity and establishes routes between nodes and itself. The authors propose a distributed algorithm for establishing and maintaining loop-free routes to the central station. They contend that a *contingency routing algorithm* (CRA) to deal effectively with topological changes affecting the primary routes (routes established by the central station) is needed. The following are attractive properties of an CRA:

(1) provides some redundancy by means of additional routes to the station. These routes can be used when the primary route fails;

(2) does not rely on instructions from the central station to establish new routes when all the existing routes of any node fail;

(3) does not employ flooding and does not create problems with excessive communication and thus collisions;

(4) ensures that each route is loop-free; and

(5) incorporates "new" links into existing routes with little overhead.

The essential idea that the authors employ in establishing routes from the nodes to the central station (dest) is one of *link reversal.* The following methods are introduced to form the basis for developing contingency routing algorithms.

- *Full Reversal Method [95]*: At each iteration, each node other than the destination that does not have any outgoing links reverses the directions of all its incoming links.
- *Partial Reversal Method [95]*: Every node i other than the destination records a list of its neighboring nodes j that have reversed the direction of the corresponding links $\tau{<}i,j{>}$. Then at each iteration each node i that does not have any outgoing links reverses the directions of the links $\tau{<}i,j{>}$ for all j which do not appear on its list and empties the list. If there does not exist such a j (e.g., the list is full), node i reverses the directions of all incoming links and empties the list.

The central station does not have to react immediately to topological changes if alternate (secondary) routes are available; however, it can intervene at any time and reestablish primary and secondary routes. The algorithms do not guarantee shortest routes and rely on the central station for periodic optimization of routing. Since there are multiple routes to the central station from any node, the contingency algorithm will be activated only when a node loses all of its available routes to the station. Even when this occurs, typically a long chain of reversals and messages will not be needed to reestablish routes. Further details can be found in Gafni and Bertsekas [95].

4.2.7 Corson and Ephremides Algorithm

Recently, Corson and Ephremides also examined the situation when the rate of topological change is not so fast as to make flooding the only alternative, but not so slow as to make the

static routing algorithms applicable [96]. They proposed a distributed algorithm to establish and maintain routes between *necessary* source-destination pairs.

The main objectives of this algorithm are to build routes only *when necessary*, to build routes *quickly* so they can be used *before* the topology changes, and to react *quickly*, establishing new routes when existing routes are destroyed. Since the essential goal of the protocol is to simply find a route, *routing optimality* is of secondary importance.

The algorithm is distributed in the sense that the nodes are only aware of the connections to their neighbors and do not have global connectivity information. The nodes also do not have global routing information. Consequently, they assume that a route through their neighbor will lead to the desired destination. The algorithm is destination-oriented, since separate versions of the protocol run independently for each destination. For simplicity, we will describe a version for one particular destination referred to as the DEST. The protocol maintains loop-free routes between desired source-destination pairs.

The protocol executes in three logical phases.

(1) *Route construction*: The construction phase builds an initial set of routes.

(2) *Route maintenance*: This phase maintains loop-free routing while arbitrary topological changes occur, rebuilding new routes only when necessary.

(3) *Route destruction*: The destruction phase ensures the erasure of any routes that may have become invalid due to topological changes.

Corson and Ephremides model the network as a graph $G = (N, L)$ consisting of a finite set of nodes N and a set of initially undirected (unassigned) links L. Every pair of "neighboring" nodes can communicate with each other in *either* direction, depending on the direction of the link. For every node i, there exists a link $\tau\langle i, j\rangle$ for every $j \in$ {neighbor of i} between

node i and neighbor j. The link $\tau\langle i,j\rangle$ may be either directed or undirected. When a link is directed from node i to node j, node i is said to be an *upstream* neighbor of node j (i is *upstream* of j), while node j is said to be a *downstream* neighbor of node i (j is *downstream* of i).

In developing their protocol, the authors assume that a packet transmitted by a node is heard by all of its neighbors. They also assume an underlying link-level protocol which ensures:

- Each node i is aware of its neighbors at all times.
- A transmitted packet is always received correctly.
- Simultaneous, two-way transmission over a link causing interference *does not occur.*

They assume that there are two broadcast channels used by the network. The first channel is to establish network control, and the second channel is for actual message transmissions. A centralized, demand-access scheme is used for each channel and functions independently within each. The access scheme is nonblocking, collision-free, and does not allow the reception of partial packets caused by arbitrary link failures and activations. This idealized scheme isolates the routing operation and provides a common basis for comparison with the routing performance of other distributed algorithms.

There are three types of control packets used in the protocol.

- **QRY:** This control packet is broadcast by a node desiring a route. It has the format [SID, DID, XID, SEQ], where SID is the source node identifier, DID is the destination node identifier, XID is the transmitting (forwarding) node identifier, and SEQ is a sequence counter. Each source keeps a separate SEQ for each destination. Hence,

the triple (SID, DID, SEQ) is a unique identifier which distinguishes a QRY from all others.

- **FQ:** An FQ is broadcast by a node that has lost *all* of its routes. The purpose of the broadcast is to inform other nodes of any invalid routes. It has the format [DID, XID], where DID and XID are as described previously.

- **RPY:** An RPY is broadcast by a node which has a route, in response to either a QRY or FQ reception. It has the format [DID, XID], where DID and XID are as described previously.

The protocol contains a timer at each node with timeout period T, which controls the time between successive QRY broadcasts. The protocol also maintains a "query-seen" array entry QS_j for each source j, which holds the source's most recently received QRY SEQ number. A single packet transmission queue is used. If the queue is full, and a new control packet must be queued for transmission, the old packet is discarded.

In the construction phase, the network is initially unassigned. Only nodes neighboring the DEST have routes to DEST, all other links being undirected. A node *has a route* if it has at least *one* downstream link; the node then believes that a path to DEST exists through the downstream neighbor. A node desiring a route to DEST broadcasts a QRY, which is "flooded" throughout network searching for nodes that have a route to DEST. Flooding here refers to a node-to-node broadcast where an individual QRY is not broadcast by a particular node more than once. QRYs travel over paths of unassigned links. When a node without a route receives the QRY, it will forward the QRY. However, nodes with a route respond by broadcasting an RPY.

An RPY is "flooded" back toward the source of the QRY. This flood is a directed flood, since RPYs travel back through network portions of undirected links. These portions are transformed into directed acyclic graphs (DAG). A directed link is created pointing toward the origin of the RPY.

The node initiating the QRY flood waits for reception of an RPY, which indicates a route has been obtained. In the process of such a QRY flood, some nodes not necessarily desiring routes, but which participated in the RPY flood, may obtain routes as well. The source node may also obtain more than one route to the DEST. The extra routes provide increased reliability. An optional metric can be used to determine a routing decision; e.g., a distance metric estimating the number of hops (transmissions) to the destination can be piggybacked on the RPY control packet. An example of the route construction phase is given in Figure 3.

The maintenance phase begins when some node looses its *last* route due to an adjacent link failure. If that node has no other nodes routing through itself, i.e., no upstream neighbors, the node broadcasts a QRY *only* if it desires a route to the DEST. The motivation for initiating this QRY flood is to replace a needed route that was lost. In Figure 4, an example of such a QRY flood is shown. If a node has other nodes routing through itself, it broadcasts an FQ *regardless* of whether or not it currently desires a route. When a node broadcasts an FQ, it not only informs its upstream neighbors not to route through it but also asks those neighbors if they have any alternate routes. The reception of an FQ over a link erases the route on that link, i.e., a directed link becomes an undirected link. As a result, all invalid routes are erased. When an upstream neighbor receives an FQ, the neighbor will first determine whether or not it still has a route. If the neighbor has an alternate route remaining, it will respond by broadcasting an RPY. However, if the FQ reception caused the neighbor to loose its last route, it will forward the FQ to any upstream neighbors. The upstream FQ propagation continues, erasing invalid routes, until either a node is found having an alternate route, or the FQ propagation halts, having erased all invalid routes, and without finding an alternate path because the network has become partioned. Figure 5 illustrates an example of invalid route erasure and path reconstruction.

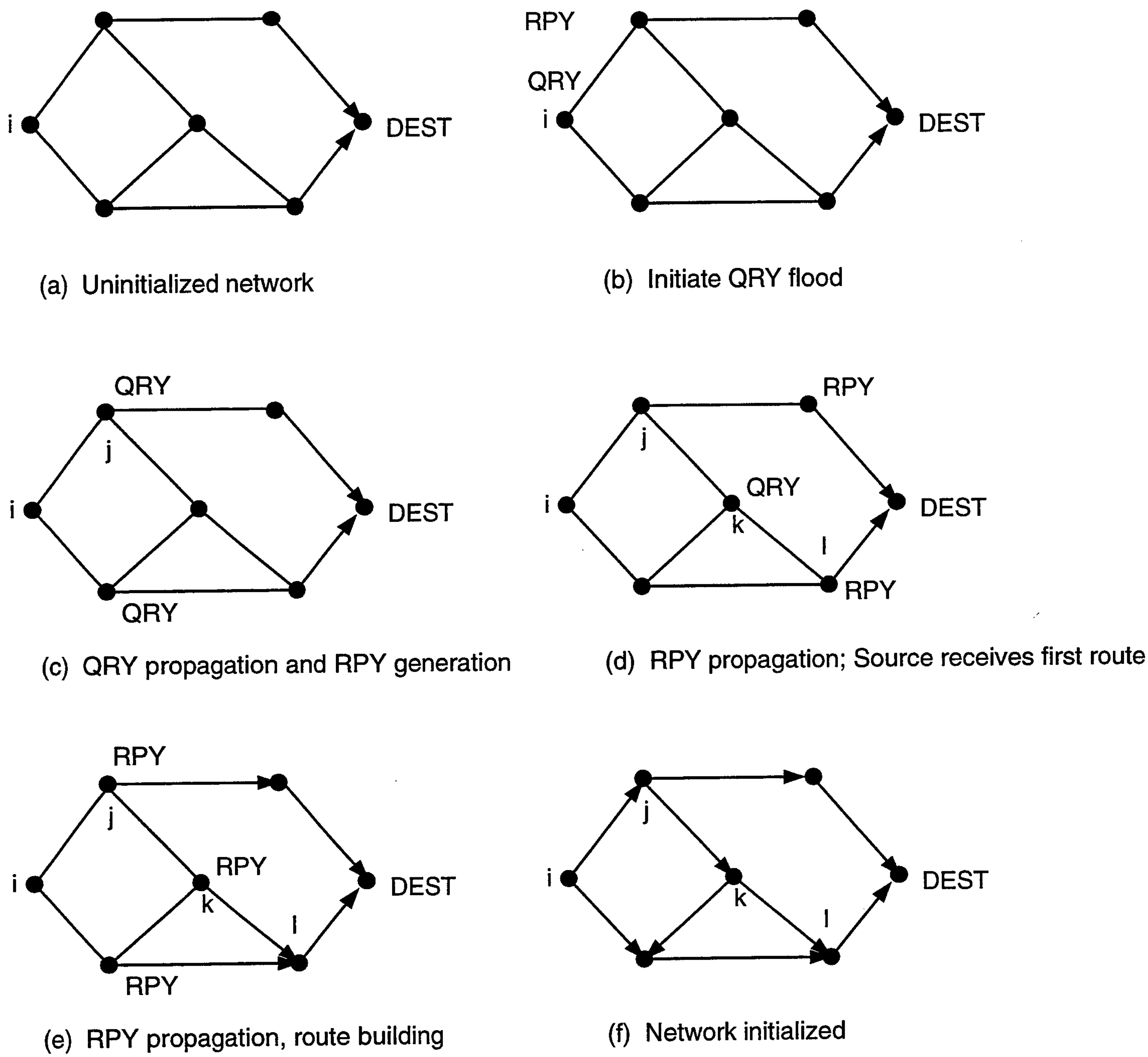


Figure 3: Example of the route construction phase of the Corson and Ephremides algorithm.

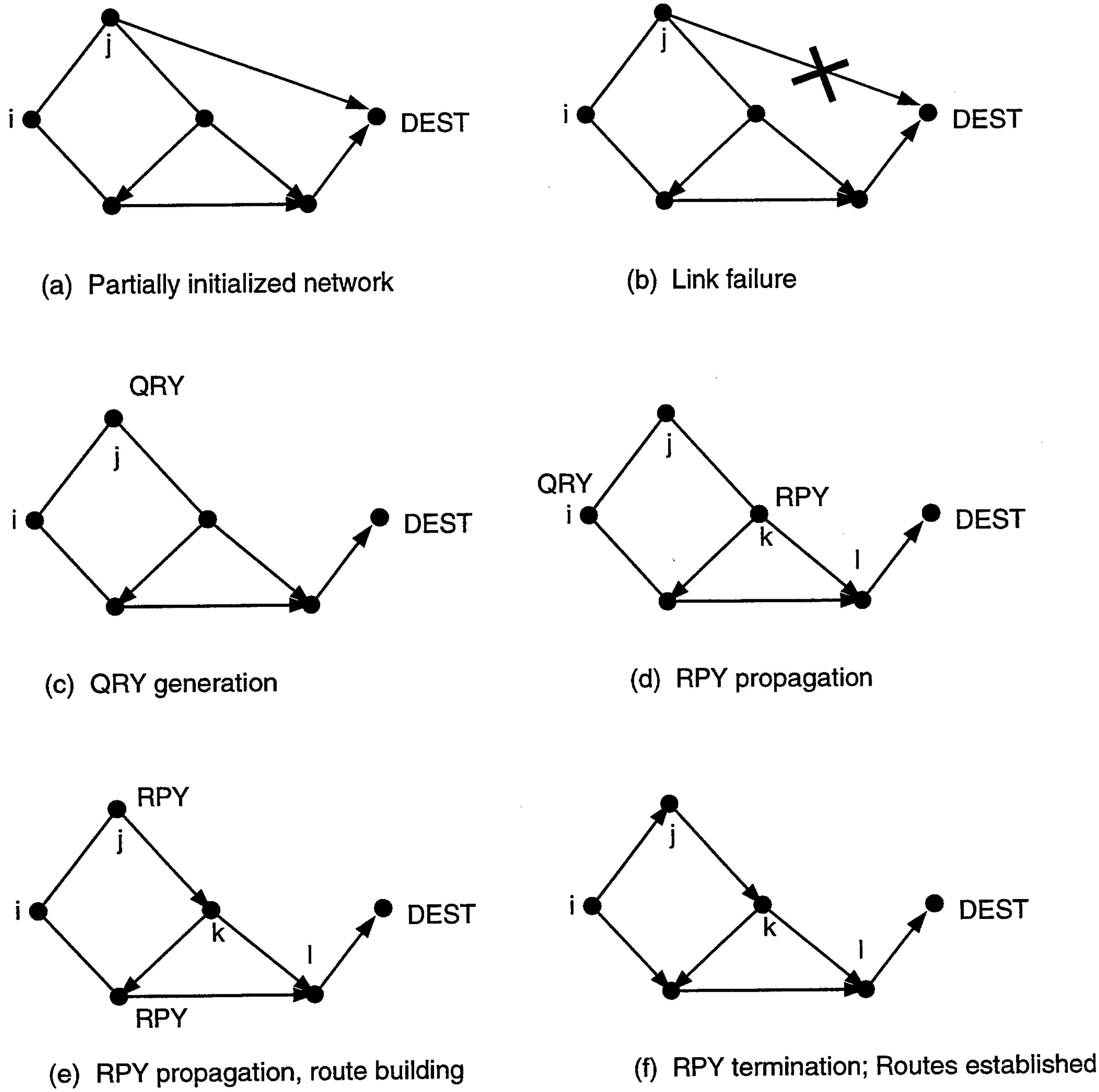


Figure 4: Example of the route maintenance phase of the Corson and Ephremides algorithm.

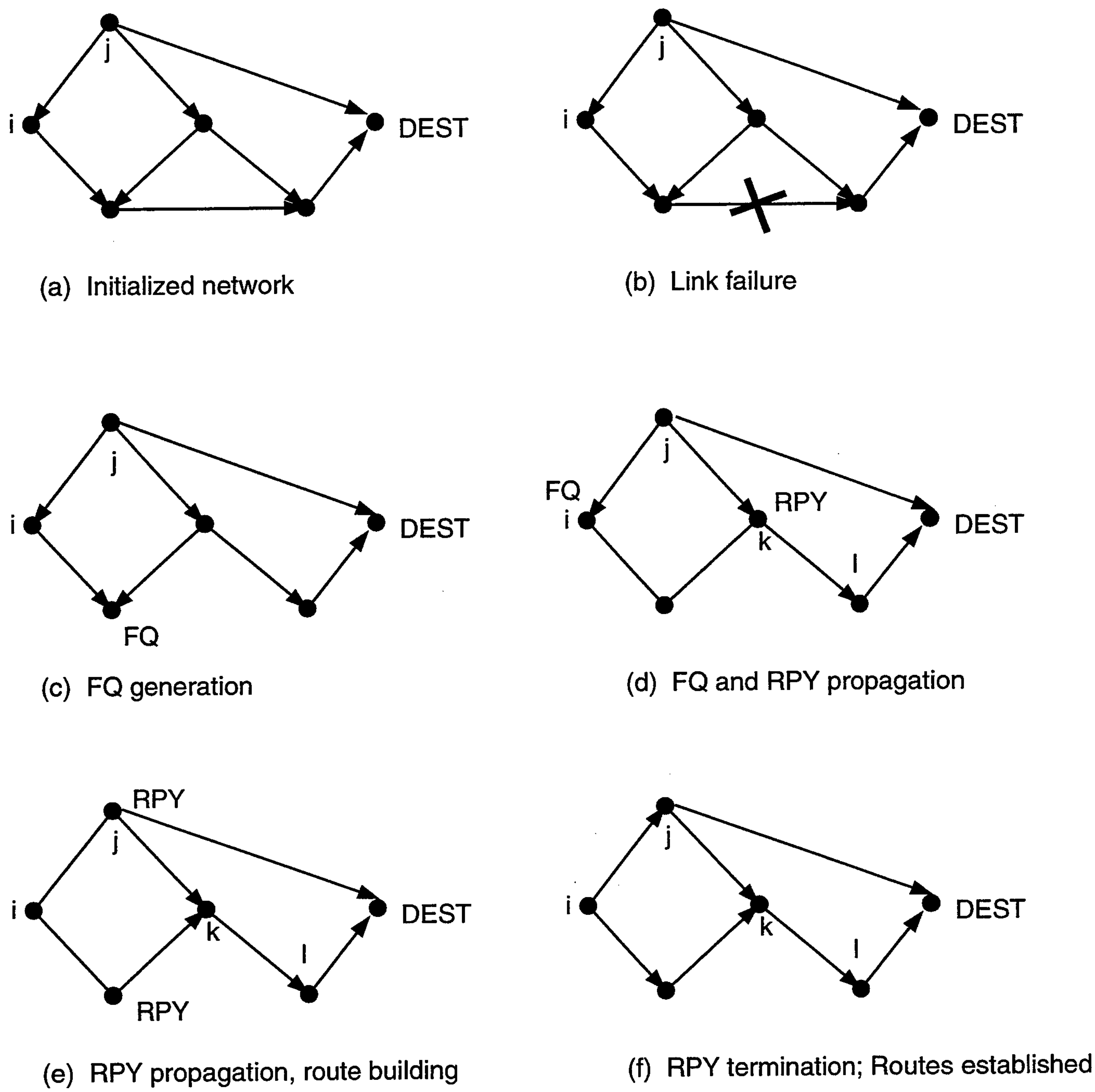


Figure 5: Example of invalid route erasure and reconstruction phase of the Corson and Ephremides algorithm.

Corson and Ephremides evaluate the performance of their algorithm by doing simulation comparisons with pure flooding and the Gafni-Bertsekas (GB) protocol [95]. Pure flooding is a distributed process of broadcasting a message throughout the network. The GB protocol, described earlier, is a distributed routing protocol that relies on sequences of link reversals to maintain routes to each destination. The authors consider two versions of their protocol:

- NP: In this version, if multiple routes are emanating from a node for the same destination, the routing choice is made randomly and uniformly among them.
- NP-SP: In this version, the distance measured in hops from the destination is piggybacked on the RPY propagation. The nodes keep an approximate estimate in a distance table ranking the relative merit of each route. Since the distance information is only carried on the RPYs and no update packets are sent when a node's shortest path estimate changes, this is not a true shortest path algorithm. The NP-SP makes routing decisions based on the estimates in the distance table and routes over the shortest path; ties are broken randomly and uniformly over the set of minimal-hop routes.

The performance measure used is *routing power*, which is defined as the ratio of the *average message throughput* to the *average message delay*. Average message throughput is the percentage of generated packets delivered to their destination during the simulation time. The average message delay is the average time spent by all messages in the network. For messages that reach their destination, the delay contribution is the complete end-to-end delay. For those packets that do not reach their destination, the delay contribution is the amount of time from generation to the end of the simulation.

For the simulation runs, the authors consider three different base topologies (see Figure 6 taken from Corson and Ephremides [96]). They model the topological changes by creating one-hop link sets and two-hop link sets for each base topology (two-hop link sets consist of those links connecting all possible node pairs two hops apart). The links are modeled by an

independent, two-state (UP/DOWN) Markovian link model, whose transition probabilities are the same for all links in that topology. In the RANDOM-12 topology model, each link independently decides whether or not to change state; both one-hop and two-hop links may be active simultaneously, and network disconnections are permitted. In the CONNECTED-12 model, both link sets are permitted to be active but the network must remain connected at all times. In the CONNECTED-1 model, only the one-hop links may be active and the network must also remain connected. State changes that violate any of the restrictions are not allowed.

The rate of topological change R, measured in link state changes per minute, is varied upwards from zero. Each node generates 1000 bit message packets according to a Poisson arrival process with arrival rate λ. Light traffic is modeled with $\lambda = 1$ packet per node per minute, while heavy traffic is captured with $\lambda = 3$ packets per node per minute. Timeout periods of $T = 1$ s and $T = 10$ s for all base topologies are examined as well as $T = 0.1$ s for base topology two.

For light traffic conditions, the simulations showed that the NP-SP version was preferable for low rates of topological change and the GB protocol was preferable for high rates of change. Since the message channel is relatively uncongested for light traffic conditions, both the speed at which routes are found and the resulting message route determine the performance. For low rates of topological change, individual routes are used for a long period of time, thus making the best routing decision an important factor. As the rate of change increases, the speed at which an algorithm reacts in the control channel becomes increasingly important. Corson and Ephremides conjecture that since the GB protocol has a lower complexity it outperforms the NP and NP-SP algorithms for light traffic and high rates of change.

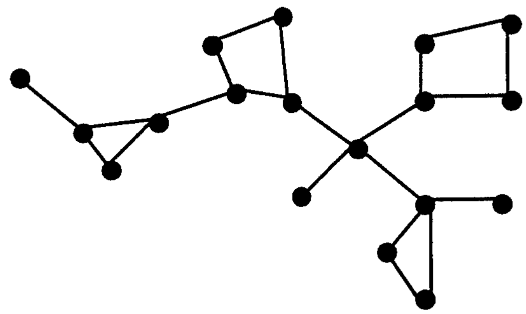
However, for heavy traffic conditions, the authors found that the NP and NP-SP protocols were preferable. At heavy traffic conditions, the message channel is highly congested, and hence the algorithm that achieves the most efficient message routing will also have the best

performance.

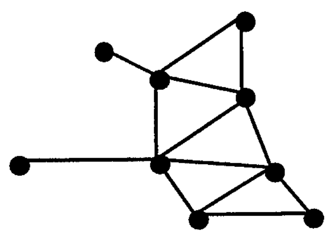
Simulations showed that the NP-SP version always outperforms the NP version of the algorithm. All protocols outperform flooding for all rates of change until the rate becomes so high that only flooding is feasible. It was found that the protocol's performance depends greatly on the value of the timeout period T. The best value of T is closely tied to the average rate of changes in the network. Depending on the value of T, the algorithm can query too often (if rate of change is low) or not often enough (if rate of change is high).

4.2.8 Humblet's Algorithm

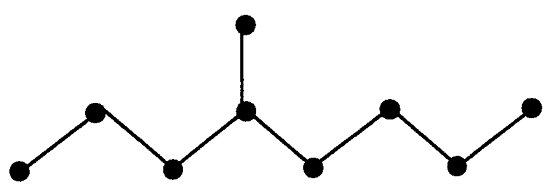
Humblet [97] proposes a distributed algorithm to compute shortest routes in a network with changing topology which uses information about the *neighbors of the destination.* The author asserts that maintaining information at node i about the neighbors of the destination is equivalent to keeping track of the entire shortest path tree rooted at node i. Briefly, the algorithm consists of two major parts. In the first part, a node observes local topological changes or it receives update messages from its neighbors. In the second part, using the information gathered, each node builds a large tree with weighted edges, where a node identity may appear more than once. Then the large tree is scanned in a "breadth-first" search to obtain a subtree, in which each node identity appears at most once. This subtree is adopted as the new "local" shortest-path tree; necessary changes with respect to the previous version are communicated to the adjacent nodes. Use of a breadth-first search of path lengths allows this algorithm to be seen as an adaptive distributed version of Dijkstra's algorithm. Further details of the algorithm can be found in Humblet [97].



(a)



(b)



(c)

Figure 6: Network topologies used in performance evaluation of the Corson and Ephremides routing algorithm.

4.2.9 Pursley and Russell: Least Resistance Routing

While a routing protocol is primarily concerned with properly guiding a transmission to its destination, it must also be robust against any interference that will be experienced by the nodes. Pursley and Russell [98] developed an adaptive, decentralized routing algorithm, *Least Resistance Routing* (LRR), which accounts for hostile jamming interference, multiple-access interference, and other partial-band interference at each of the other nodes in the network. In this algorithm, each node maintains a measure of its *own* reception quality for the packet transmissions coming from its neighbors. This measure is passed along the network on data packets and on special control packets called Packet Radio Organization Packets (PROPs) [92]. The metric for LRR accounts for the channel conditions *as seen by a frequency-hop receiver* (FH); it is designed to capture the way that interference *encountered* at the FH radio receiver affects network performance [99, 100].

The authors consider a static network topology in which jamming is dynamic. The nodes within the network use time-slotted, receiver-directed FH spread-spectrum signaling. Hence, a node must know the identification of the intended receiver, as well as the receiver's FH pattern. The PROPs are transmitted using a common hopping pattern, so all nodes within range of the transmission can potentially receive the packet (all nodes use omnidirectional antennas). As a result, the only mechanism a node has for distinguishing between transmissions is due to the different FH patterns used by the various transmitting nodes.

In the LRR algorithm, each node forms an *interference statistic* for each of its frequency slots. This statistic may be based on predetection information, such as energy levels, or postdetection information such as quality information from the demodulator, or both [101]. The vector of statistics is denoted by $\xi = (\xi_1, \xi_2, \cdots, \xi_q)$, where ξ_i is the interference statistic for the ith frequency slot, and q is the total number of frequency slots. ξ_i is a combination of all types of partial-band interference. The version of LRR presented in Pursley and Russell [98] does not distinguish between the various types of partial-band interference.

The interference statistic ξ_i is then mapped into an interference factor $f(\xi_i)$ by means of a function f. For example, if ξ_i is a measure of the interference power in the ith frequency slot, then the most elementary function for this purpose is a simple threshold function: $f(\xi_i) = 0$ if $\xi_i \leq \Lambda$ and $f(\xi_i) = 1$ if $\xi_i > \Lambda$. The interference factors can then be combined in a number of ways to a single *interference measure* I. For instance, the average of the interference factors for the q frequency slots is

$$I = q^{-1} \sum_{i=1}^{q} f(\xi_i). \tag{22}$$

In this case, I is just the ratio of the number of frequency slots with interference above the threshold to the total number of frequency slots.

Estimates of the conditional probability of error and the conditional probability of erasure can be obtained from the interference measure. The probability of acquiring synchronization P_A and the probability of decoding correctly (given that synchronism has been acquired), $1 - P_E$, can be calculated from I. For further details, see Pursley and Russell [98].

A node can receive a given packet if it is not transmitting and if it has not already acquired a different packet first. When a node is in the receive mode, and is not in the process of receiving some other packet, the conditional probability that it will receive a packet correctly is $P_R = P_A(1 - P_E)$. The resistance at the node is defined as

$$W = -\log P_R, \tag{23}$$

which is known as the log-probability (LP) metric. The resistance for a path is defined as the sum of the resistances of each link.

In more sophisticated versions of LRR, other information can be used to determine a node's resistance, such as the number of packets in the node's buffer, the recent history of traffic near the radio, and an erroneous symbol count from packets previously received by the radio. This information can be combined with the node's resistance using suitable weighting factors. For instance, if $E(A, B)$ denotes the relative frequency of errors in recent

transmissions from node A to node B, the resistance of the link from A to B can be defined by

$$R(A, B) = \alpha W_B + \beta E(A, B), \tag{24}$$

where α and β are coefficients selected to give the desired emphasis, and W_B is the resistance at node B.

In the simulation in Pursley and Russell [98], the FH nodes are grouped into three categories: (1) FH nodes that are interacting closely in a local network, referred to as a *subnetwork*, (2) FH nodes that are not part of the subnetwork, and (3) other FH nodes. While all the nodes contribute interference in the subnetwork, only the nodes within the subnetwork interact in the routing protocol. The model used is illustrated in Figure 7 (taken from Pursley and Russell [98]); the *subnetwork* consists of the nodes numbered 1−12. A significant amount of traffic will flow through the subnetwork, entering via nodes 5−8. The traffic generated at nodes 5−8 represents traffic originating at these nodes together with traffic that is routed through these nodes from the other nodes that are not part of the subnetwork. Consequently, the packet generation rates for nodes 5−8 are twice those for the other nodes in the subnetwork.

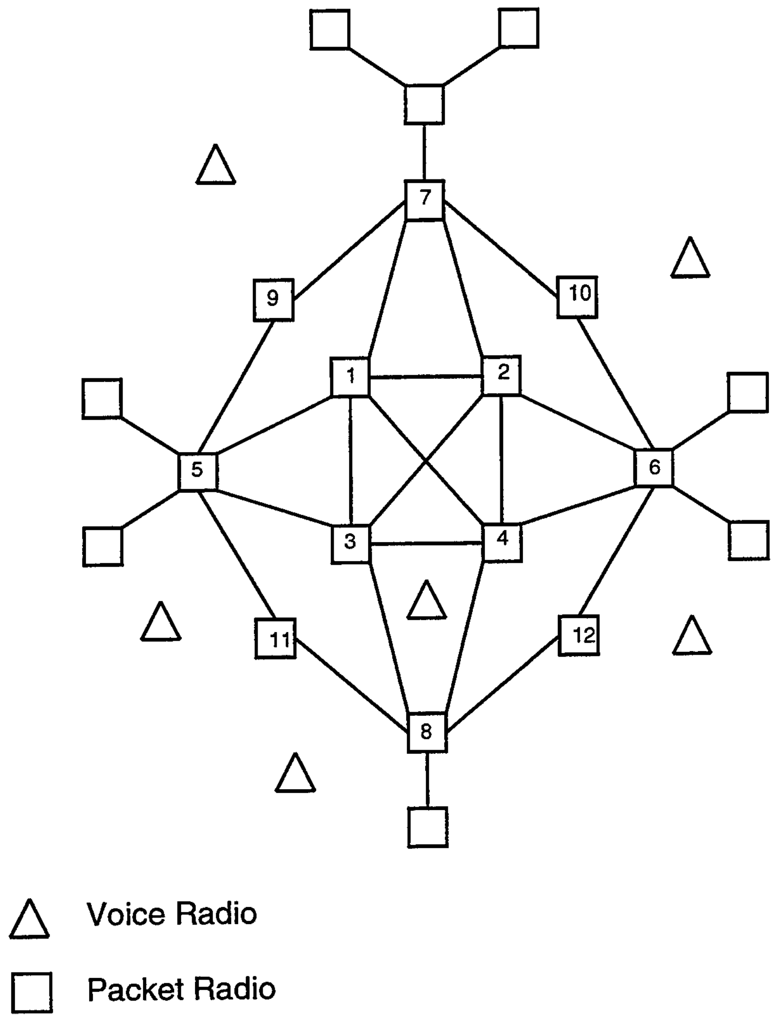


Figure 7: Model for the packet radio network topology: subnetwork consists of nodes 1–12.

The interference statistics for the subnetwork nodes are determined during the packet intervals when the node is not transmitting. The link resistances are computed, and the necessary path resistances are updated by using a Bellman-Ford type algorithm. The path resistance values are spread throughout the network by three methods: (1) each node includes its current interference factor in the header of each data and acknowledgment packet that it transmits, (2) when a node acknowledges a packet, it includes in the acknowledgment packet the path resistance to the destination for that packet, or (3) by using PROP transmissions.

For each destination, each node stores a table containing the outgoing links for the two routes with the lowest resistance values. Then, at a particular node, a packet is forwarded on the outgoing link for the route with the least resistance to the packet's destination. This link is referred to as the *primary* link, and as many as three attempts to forward the packet on this link are permitted. If none of the attempts is acknowledged, then the next three forwarding attempts are made on the outgoing link with the next lowest resistance to the destination. This link is referred to as the *secondary* link. If the node has only one outgoing link to the destination, then all six attempts are made on that link. A packet is discarded after six unsuccessful forwarding attempts are made.

Using simulations, Pursley and Russell measured the performance of the LRR protocol by *marking* certain packets and monitoring their flow through the network. (For further details see Pursley and Russell [98].) The performance of the LRR was analyzed by examining three measures: *end-to-end throughput*, *end-to-end probability of success*, and *end-to-end delay*. The *end-to-end throughput* is defined as the average number of marked packets that reach their destinations per packet interval. The *end-to-end probability of success* is defined as the average fraction of marked packets that reach their destinations. The *end-to-end delay* is defined as the average number of packet intervals required for *marked* packets to arrive at their destinations. Discarded packets were not counted in the end-to-end delay. Consequently, the end-to-end delay defined is a meaningful performance measure only when the end-to-end probability of success is high.

For an interference environment corresponding to partial-band jamming of 55% of the band, the success rate is about 20% for the transmissions to a receiver that is jammed. For an interference environment where 40% of the band is jammed, approximately 50% of the transmissions to a jammed node are successful. Since jamming of a larger fraction of the band effectively removes the jammed node from network activity, it was not considered. From the results of various simulation runs, it was observed that the LRR algorithm adapts quickly to a change in the position of a mobile jammer [98].

4.2.10 Pursley and Russell: Adaptive Forwarding

In an another paper [102], Pursley and Russell examined adaptive protocols for forwarding around localized partial-band jamming in a frequency-hop packet radio network. They focused attention on routing changes that a node can make to its normal routing pattern when a partial-band jammer appears nearby. The routing changes occur in the time periods between routing table updates in a network with dynamic routing. The resulting changes in the transmission paths only affect the routes near the jammer; the protocol only requires local information for its execution.

Pursley and Russell consider particular forwarding protocols and evaluate the performance of these protocols through simulation studies. Again, they consider a *subnetwork* of a packet radio network, shown in Figure 8 (taken from Pursley and Russell [102]), and monitor the progress of packets in the subnetwork. The subnetwork consists of the radios in the network that are near the source of the partial-band jamming, i.e., nodes $1-8$ in Figure 8. While the nodes in the network contribute to the traffic in the subnetwork and are a source of interference, the radios outside the network contribute interference only. The traffic outside the subnetwork that routes through the subnetwork is captured by the traffic "generated" at nodes $5-8$. Hence, the traffic generated at these nodes represents traffic originated at these nodes together with traffic from outside the subnetwork that is routed through these nodes. Again, the authors are concerned with static network topologies with dynamic

network jamming; the network assumptions made are similar to those in Pursley and Russell [98], as described earlier.

The nodes in the subnetwork forward packets on one of the shortest-length paths from the source to the desired destination. If there are more than one outgoing links at a node on the shortest-length routes, one of the outgoing links is labeled the *primary* outgoing link, and the other is labeled the *secondary* outgoing link. The forwarding protocol then determines on which one of these links to transmit a packet. The node is limited to six transmission attempts for a particular packet; after six unsuccessful attempts at one node, the packet is discarded. In variations of this protocol, a parameter m is used, where m is the maximum number of consecutive unsuccessful attempts for a given packet and a given outgoing link. After m attempts on a particular outgoing link, the forwarding protocol selects a different outgoing link and attempts the remaining $(6 - m)$ transmissions.

Pursley and Russell examined two classes of forwarding protocols: the *primary-path forwarding protocols* and the *good-link protocols.* The *primary 6/m* protocol forwards the packet for the initial m attempts on the primary link; for $m = 6$, all attempts are on a node's primary outgoing link, while for $m = 3$, if the first three forwarding attempts have been unsuccessful, the node will then use its secondary outgoing link. The *good-link 6/m* protocol uses stored information about the link that was *last* used *successfully.* It combines this information with the current feedback from the acknowledgment packets, to make a routing decision. Initially, a packet is forwarded on the link that was used for the previous packet with the same destination, *provided* that previous packet was transmitted successfully. This link is used for the the first m transmission attempts, if that many are required. If the m transmissions were unsuccessful, the protocol then switches to the alternative link for the next m transmission attempts. For example, if $m = 2$ and the first two attempts were made unsuccessfully on the secondary link, then the next two attempts will be made on the primary link, and the final two attempts will be on the secondary link again.

For performance simulations, the authors consider four jamming scenarios. First, a fixed-

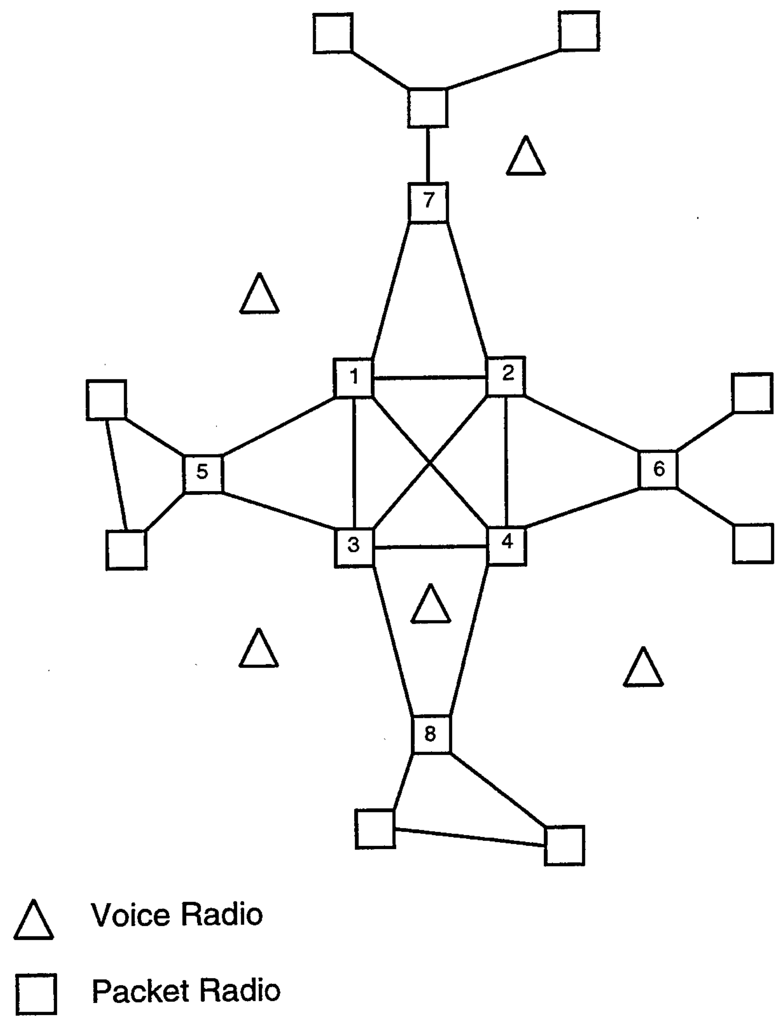


Figure 8: Model for the packet radio network topology: subnetwork consists of nodes 1–8.

location jammer that interferes with transmissions to node 1 only is considered. In the next three scenarios, the jammer moves between nodes 1 and 3. Different jamming *periods* are simulated, where a period is the number of packet intervals the jammer is located at a node before it moves to another node. Various packet generation probabilities are also considered. The remaining simulation parameters and performance measures are similar to those used in Pursley and Russell [98] as described earlier.

For the fixed jammer case, the good-link protocols have the highest throughput and end-to-end success probabilities for each packet generation probability. The primary 6/6 protocol has the lowest throughput and the lowest end-to-end success probabilities. In general, for the stationary jammer, the forwarding protocols that used secondary routes performed better than those that used fixed routes. For the mobile jamming cases, the good-link 6/3 protocol has slightly greater throughput than the primary 6/3 protocol. Again, the primary 6/6 protocol still has much poorer performance, *except* at the highest packet generation probability. Also, the good-link protocols perform best for the stationary jammer and their performance decreases as the jammer period decreases. The performance of the primary 6/3 forwarding protocol does not depend on the jammer period since this protocol does not store any information from the past. However, it was found that for the primary 6/6 protocol, there is a dramatic change in the throughput and success probabilities as the jammer period changes. In general, the performance of all of the forwarding protocols becomes similar as the jammer period decreases.

Overall, the good-link forwarding protocols have the best performance of the protocols considered. Significantly better performance is further obtained from the forwarding protocols that use secondary routes if the initial transmission attempts were unsuccessful.

4.2.11 Pursley and Russell: Side Information

Pursley and Russell further extended the aforementioned forwarding and routing protocols for slow-frequency hop (SFH) packet radio networks to include *side information* [103]. Side information can be extracted from received signals that are subject to noise and interference and can be used to enhance the network protocols. In the literature, several methods have been considered for extracting side information; a method that uses *test symbols* was found to be the most suitable for application to network protocols [104]. In this method, a known sequence of symbols, called test symbols, is included in the information symbols stream for each dwell interval. The number of symbols received correctly during a dwell interval serves as a statistic to determine the reliability of the data symbols in that dwell interval. Increasing the number of test symbols increases the reliability of this method; however, this also decreases the information rate. Consequently, a tradeoff can be exercised to maximize the information throughput subject to the error probability requirements.

Information about the interference environment at a receiver is provided by the side information available at the decoder. Each radio maintains a measure of its own reception quality, which is determined by the choice of *metric.* The metric should accurately reflect the radio channel *as seen by a frequency-hop receiver.* The authors examine three different metrics in their simulations:

(1) Log-probability (LP) metric - This metric is used in Pursley and Russell [98] and was described earlier. It is based on perfect knowledge of the interference environment at a receiver.

(2) Error and erasures (EE) metric - This metric is the number of erasures plus twice the number of errors from a successfully acquired packet at a receiver. The radio's resistance is the EE metric for the last successfully acquired packet.

(3) Error and erasures with acknowledgments (EEA) metric - This metric is similar to the EE metric, except now each time a radio sends a packet to a neighbor and does not

receive an acknowledgment, the radio will increment the stored resistance value for that neighbor by one.

Through simulations, Pursley and Russell examine the previously described forwarding protocols (primary n/m and good-link n/m) and the routing protocol (LRR protocol), using the different metrics. They use the notion of a subnetwork as described previously for the LRR simulations (see Figure 7 taken from Pursley and Russell [98]). They calculate various conditional probabilities for a packet to be decoded in the presence of both partial-band and multiple-access interference and use these probabilities to simulate channel conditions and network behavior. Further details can be found in Pursley and Russell [103]. The remainder of their simulation setup and performance measures are identical to those described previously for Pursley and Russell [98].

The authors examined the forwarding protocols for various levels of partial-band interference, multiple-access interference, wideband noise, signal-to-noise ratios, and various jammer periods. The simulations found that the EEA-based forwarding protocol gives higher throughput for some of the packet generation probabilities compared to the good-link protocol. Also, EEA-based forwarding is superior to the EE-based forwarding. When the signal-to-noise ratio is large, the side information and the information on lack of acknowledgments indicate the reliability and quality of a link. However, for lower signal-to-noise ratios, it was more difficult to determine if a failure to receive an acknowledgment was due to partial-band interference or to thermal noise alone. The authors found that in most cases the throughput was lower for a larger jammer period. As expected, the forwarding protocols do not offer the best solution to long-term changes in the network.

The LRR protocol with the different metrics was examined and the simulations showed that the LP metric does not have the best network performance of those metrics investigated. This can be attributed to the fact that while the LP metric uses perfect knowledge of the interference environment, it does not account for any other factors that affect the probability

that a radio can receive a transmission, e.g., likelihood that the receiver is busy. Overall, the EEA metric most accurately characterizes the conditions as seen by a frequency-hop receiver. Side information is beneficial in selecting routes that avoid parts of the network that have excessive interference; the acknowledgment information is effective in eliminating outdated routing information. It was also found that the routing protocols are not particularly sensitive to variations in the jammer period. For detailed simulation results, see Pursley and Russell [103].

4.3 Distance Vector and Link-Vector Algorithms

Distance vector routing algorithms are particularly attractive because of their parallel processing capability. The basic computation step in a distance vector algorithm can be executed in parallel at each node. The parallel nature of distance vector algorithms make them ideal for supporting the aggregation of destinations by reducing communication, processing, and storage overhead. In distance vector algorithms, nodes exchange information on path characteristics, not on link or node characteristics.

4.3.1 Awerbuch, Bar-Noy, and Gopal Algorithm

Awerbuch, Bar-Noy, and Gopal [94] examine a distance vector algorithm and propose two modifications to the distributed Bellman-Ford algorithm, which result in a polynomial message complexity (as compared to the exponential message complexity of the DBF). As described previously, the DBF consists of two basic rules: the adopting rule and the sending rule. The authors propose modifications to the adopting rule.

- *Multiplicative Adopting Rule (MAR)*: Suppose node x, with label $b(x)$, receives $b'(x)$ from node z. If $b'(x) < b(x)/\alpha$, then node x adopts $b'(x)$ and sets the value of *parent*(x) to z. When $\alpha = 1$, this algorithm is just the DBF.

- *Additive Adopting Rule (AAR)*: Suppose node x, with label $b(x)$, receives $b'(x)$ from node z. If $b'(x) < (b(x) - \beta)$, then node x adopts $b'(x)$ and sets the value of $parent(x)$ to z. When $\beta = 0$, this algorithms is just the DBF.

The authors provide various propositions to exhibit the polynomial time complexity and message complexity of the routing algorithms resulting from the previously mentioned adopting rules. Further details are provided in Awerbuch, Bar-Noy, and Gopal [94].

4.3.2 Garcia-Luna-Aceves Algorithm

Another modification to the distributed Bellman-Ford Algorithm is provided by Garcia-Luna-Aceves [105]. In this algorithm, each node maintains in its routing table the next hop (successor) and shortest distance in number of hops of the paths to each destination. A node sends update messages only to its neighbors; these messages contain the length in hops of the selected path to the destination. A node always chooses new successors that are at most equidistant, i.e., same distance or closer, to the destination than the node's current successor to the same destination. The algorithm avoids loops by requiring that a node does not send an update message before it receives replies from all its neighbors to the previous message.

In this algorithm, when node i processes an update message from a neighbor and needs to update its routing table for a given destination j, or detects a change in cost or availability of a link, node i tries to secure a new "feasible" successor with the shortest distance to node j. For node i, a "feasible" successor toward node j is a neighbor node that has reported a distance to the destination that is the same or closer than the distance reported by the current successor of node i. The algorithm behaves the same as a distributed Bellman-Ford algorithm when feasible successors are found. However, when a node i cannot find a feasible successor with the shortest distance to node j, node i freezes its successors to node j and sends an update message to all of its neighbors. Node i cannot send another update message until it has received replies from all its neighbors to the message it has just sent. Garcia-

Luna-Aceves asserts that the proposed algorithm eliminates *all* the looping problems of the Bellman-Ford algorithm. For further details see Garcia-Luna-Aceves [105].

4.3.3 Behrens and Garcia-Luna-Aceves Algorithm

An interesting modification of link-state algorithms is link-vector algorithms. Link-vector algorithms function by selective spreading of link-state information based on the computation of preferred paths [106]. This is in contrast to link-state algorithms, which rely on flooding of complete link-state information to all nodes. Link-vector algorithms are primarily used for the distributed maintenance of necessary routing information in large networks.

Behrens and Garcia-Luna-Aceves [106] present a link-vector algorithm whose essential idea consists of requiring each node to forward to its neighbors the characteristics of each of the links it uses in reaching a destination through one or more preferred paths. Each node also reports to its neighbors which links it has erased from its preferred paths. Each node constructs a *source graph* using this information and a *path selection algorithm.* A path selection algorithm can be shortest path, such as Bellman-Ford algorithm, Dijkstra's algorithm, maximum-capacity path, or any other comparable algorithm. A source graph for a node consists of all the links the node uses in the preferred paths to each destination. Consequently, a node has topology information consisting of its adjacent links and the source graphs reported by its neighbors. By running a local algorithm on its source graph, a node derives a routing table, which specifies the next node (or nodes) or paths to each destination. A source graph is reported by a node to its neighbors in an incremental manner. A node sends an *update* (a message indicating change in topology) only when a link is modified, added, or deleted in its source graph. Thus, the algorithm avoids the flooding inherent in link-state algorithms. For details, see Behrens and Garcia-Luna-Aceves [106].

5. State-of-the-Art

In this section, we survey the state of the art in wireless data networks. This is done to provide a view of current advances in the development of civilian packet communication systems. While the wireless data systems described here are not directly applicable to a battlefield environment, they share important common features with tactical packet radio networks. Where appropriate, we have highlighted these common features.

The latest trends in wireless information networks are evolving around either (1) data-oriented networks such as Wireless Local Area Networks (WLANs) and Mobile Data Networks or (2) voice-oriented applications such as digital cellular, cordless telephone, and wireless PBX [107]. (Figure 9 provides a general overview of the different categories in wireless information networks.) Mobile data networks usually operate at low data rates over urban radio channels, using familiar multiple-access methods. The essential goal in these networks is to develop a system that makes efficient use of available bandwidth to serve a large number of users that are spread out over wide geographical areas. A WLAN typically serves a limited number of users in a well-defined indoor area; system factors such as overall bandwidth efficiency and product standardization, are not crucial. However, the achievable data rate is an important issue in selecting a WLAN, and hence, the transmission channel characteristics are important issues. While the channel access methods and network topologies used in a WLAN are similar from one system to another, the transmission technologies can vary widely. In the literature, local high-speed data communication systems are referred to as WLANs, and low-speed wide-area wireless data communication is called *mobile data.*

5.1 Mobile Data Networks

Presently, mobile data services provide length-limited wireless connection with in-building penetration to portable user terminals in metropolitan areas. The transmission rates of these systems are comparable to voice-band modem rates (up to 19.2 kbits/s). There typically is

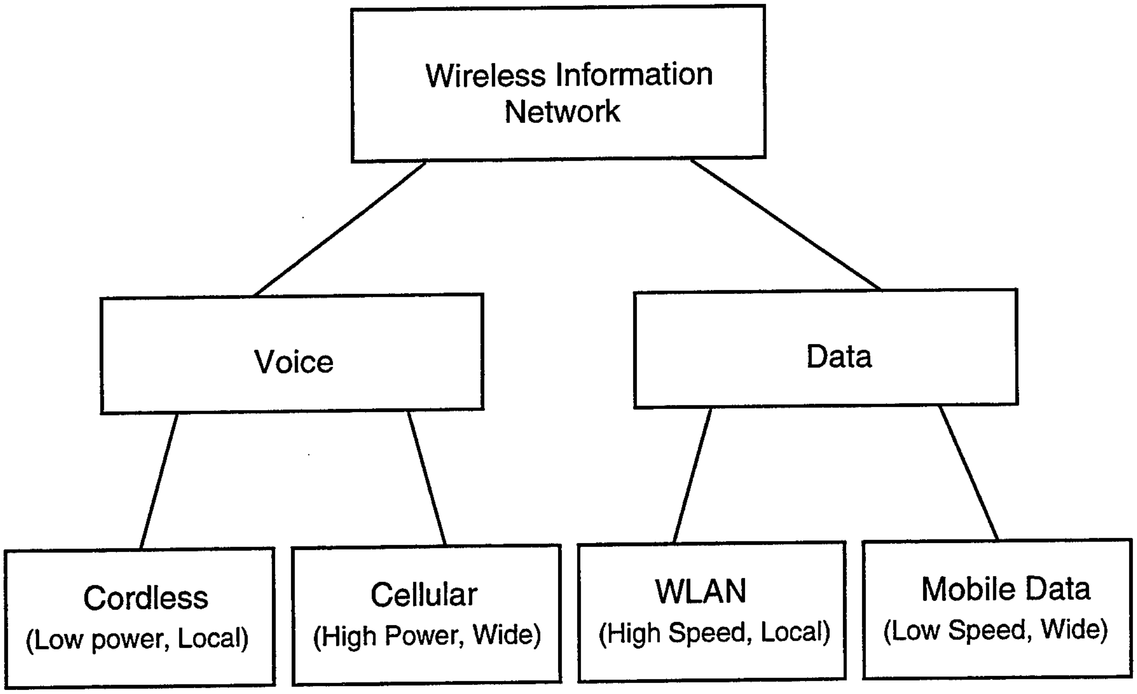


Figure 9: Categories of wireless information networks.

a limitation on the size of the file that can be transmitted in each communication session. Since mobile data users generally use portable units inside a building and in a stationary location, in-building penetration is an essential feature of these services.

Packet data services currently available for mobile applications include (1) ARDIS, formed by IBM and Motorola, and (2) RAM Mobile Data Network, which uses Ericsson MOBITEX data technology. Currently, Cellular Digital Packet Data (CDPD) is awaiting introduction into the market. CDPD is being designed to transport data as a supplementary service overlaid onto existing analog cellular telephone networks.

5.1.1 ARDIS

ARDIS is a two-way radio service first developed in 1983. ARDIS consists of four network control centers with 32 network controllers distributed through 1,250 base stations in 400 cities in the United States. This service is well suited for two-way transfer of data

files less than 10 kbytes in size. A major portion of its use is in support of computer-aided dispatching, such as that used by field service personnel while on sight. Remote users can access the system from lap-top radio terminals that communicate with the base stations. The operating frequency of ARDIS is 800 MHz, and the RF links use separate receive and transmit frequencies that are 45 MHz apart. The system uses an RF channel data rate of 9.6 kbits/s, with a user data rate of about 8,000 bits/s. The system architecture is cellular; the cell coverage areas overlap to increase the probability that signal transmission from a portable transmitter will reach *at least one* base station. While the portable units operate with 4 W of radiated power, the base station power is 40 W to provide LOS coverage up to a 10–15-mile radius. The modulation technique used in ARDIS is frequency-shift keying (FSK). The channel access method is frequency-division multiple access (FDMA), and the transmission packet length is 256 bytes.

5.1.2 MOBITEX

The MOBITEX system is a nationwide interconnected, radio network which first went into operation in Sweden in 1986. Other networks were implemented in Norway, Finland, Canada, United Kingdom, and the United States of America. The MOBITEX is an intelligent network with an open architecture that allows the establishment of virtual networks. The network architecture is hierarchical; at the top of the hierarchy is the Network Control Center (NCC) from where the entire network is managed. The MOBITEX system, similar to the ARDIS, also uses packet-switching techniques to allow multiple users to access the same channel at the same time. The message packets are switched at the lowest network level. When two mobile users in the same service area need to communicate with each other, their messages are relayed through the local base station. The base stations are laid out in a grid pattern with the same system engineering rules as those used for cellular telephone systems. The MOBITEX system actually operates in much the same way as a cellular telephone system, with the difference being that handoffs are not managed by the network, i.e., when a radio connection is to be changed from one base station to another. The handoff decision is

not made by the network computer as in cellular telephone systems, but rather by the mobile terminal itself. The base stations transmit at $935-940$ MHz, while the mobile units transmit at $896-901$ MHz. There are about $10-30$ frequency pairs used in each service area. The system uses dynamic power settings, roughly 100 mW - 4 W for portable units and 100 mW - 10 W for mobile units. The Gaussian Minimum Shift-Keying (GMSK) modulation technique is used, with noncoherent demodulation. The transmission rate is $8,000$ bits/s half duplex in 12.5 kHz channels; the service is suitable for file transfers up to 20 kbytes. The packet size is 512 bytes with a delay of $1-3$ s. To ensure the bit-error-rate quality of delivered data packets, forward-error-correction and retransmissions are used. The system uses the dynamic slotted-ALOHA random-access method.

5.1.3 CDPD

The Cellular Digital Packet Data (CDPD) system provides packet data services in an overlay to the existing analog cellular telephone network. An underlying goal of the CDPD system is to not interfere with the existing cellular telephone services; the system should provide data services on a noninterfering basis using the same 30 kHz channels. In essence, the system is designed to use the cellular channels that are not being used for voice traffic and to switch channels when the current channel is allocated to voice service. The compatibility with the existing cellular telephone system allows CDPD to be installed in any analog cellular system. Consequently, the data services provided are not dependent upon support of a digital cellular standard in the particular service area. While CDPD cannot actually increase the number of usable channels in a cell, it can provide an overall gain in user capacity, i.e., if data users use CDPD instead of voice channels. The structure of a CDPD network is similar to the structure of the cellular network with which it shares channels.

5.2 Wireless LANs

The existing technologies for WLANs are (1) unlicensed spread-spectrum systems operating in ISM bands [108], (2) licensed cellular systems operating at 18–19 GHz [109], and (3) diffused and directed-beam infrared (IR) systems [110]. Diffused IR LANs offer moderate data rates and coverage, and thus are suitable for moderate-size offices, short-distance battery-oriented applications, and environments subject to radio interference. Directed-beam IR is suitable for large-file transfers between main frames and servers, as well as large open offices with many fixed terminals. (It provides higher data rates with reasonable coverage for applications employing fixed terminals.) WLANs at tens of GHz are suitable for high-speed communications in large partitioned areas, e.g., larger offices or similar open areas such as libraries. The spread-spectrum systems offer the largest coverage and are well suited for applications where penetration through building floors is required, e.g., small business applications where terminals are distributed over several floors of a building. The next generation of WLANs involves designs to be incorporated into lap-top, notebook, and pen-pad computers, where significant reductions in size and power consumption are required.

In WLANs, only the simplest modem techniques have been adopted thus far. However, as the market for portable data terminals, notebook computers, etc., grows, the resulting demand for higher data rates for WLANs will also grow. Consequently, there will be a migration of more sophisticated wireline modem technologies into WLAN products. Estimated data rates of 1 Mbit/s are the low end of the range of data rates achievable for WLANs. Data rates can be increased by (1) employing modulation and coding techniques yielding greater bandwidth efficiency, (2) using diversity reception techniques and sectored antennas, (3) using multirate modems, (4) implementing adaptive equalization techniques at the receiver, and (5) using multitone modems.

Spread-spectrum technology for the WLAN industry has the important feature that the antimultipath and antiinterference nature of the technique increase the coverage and re-

liability of the modem. ISM band availability is the prominent reason for development of the spread-spectrum wireless LAN products. Bandwidth of 26 MHz is available in the 902 − 928 MHz ISM band, with a minimum bandwidth expansion factor of 10. WLAN product designers of this band typically sacrifice bandwidth expansion for achieving higher data rates. Consequently, a data rate of around 2 Mbits/s can be achieved with a simple QPSK modem. The spread-spectrum devices operating in the 910 MHz band can cover several floors of a building. The ISM bands at higher frequencies provide wider bandwidths and, hence, higher data rates.

Presently, an important consideration for the WLAN industry is to provide services for portable consumption in order to give satisfactory battery-powered service. Slow FH in the ISM bands is being considered for this purpose. There are three basic topologies that are commonly used in local wireless networks: centralized, distributed, and multihop configurations. In the centralized structure, one station (C) serves as the hub of the network and user stations are located within the *area*. Any communication between users goes through the hub. Essentially, the hub station controls the user stations and monitors each user's transmissions. A major advantage of the centralized topology is that the network can be designed to operate with efficient use of signal transmission power. One disadvantage of this topology is the existence of a single failure point, namely the hub.

In a distributed network, all terminals communicate with one another directly. The peer-to-peer capability of this structure provides instant connectivity without the need for a central controller. In the existing WLANs, distributed network configurations are not as widely used as centralized configurations. However, many ultrahigh-frequency (UHF) and small very-high-frequency (VHF) land mobile networks are distributed networks, e.g., fleet dispatch and public safety communications. In this topology, a server node provides the connection to a *backbone* network, serving as a bridge or gateway. An important advantage of the distributed network is the absence of a single point of failure. Also, the messages do not suffer the store-and-forward delay that is characteristic of centralized networks. A disadvantage of this topology is the absence of a central unit controlling power or timing in

the network.

In a multihop network, users communicate with one another by transmissions traversing multiple links in the network. Consequently, this topology offers the best user-to-user connectivity among all the topologies. Power efficiency is a major advantage in the multihop network. This stems from the fact that message transmission between widely separated users is done with multiple shorter hops. In some networks, such as military tactical communication over a wide operational area, multihop networks provide the only practical and reliable approach to connectivity among mobile users, e.g., the U.S. Army Mobile Subscriber Equipment (MSE) network [111, 112]. Connection to a backbone or other networks is accomplished by equipping one or more nodes with the necessary connection capability. As a result, one disadvantage of the multihop network is the added complexity to implement efficient message routing and control algorithms. Another disadvantage of this topology is the accumulated store-and-forward delay incurred by multiple hops connecting widely separated users. Multihop networks have provided applications in military radio, public safety communications, and other packet radio networks [14]. However, they have not yet been adopted in the wireless LAN industry.

6. Conclusions

This report has surveyed various approaches and protocols used for routing information through mobile packet radio networks. Of particular interest in this report were networks that exhibited dynamically changing topologies. We have focused on issues that reside within the lower three layers of the standard OSI network architecture model, such as network organization, channel signaling and media access, link scheduling, and routing. Where available, performance evaluations of packet radio networks were also included.

Our investigation of the previous issues has suggested the following conclusions.

(1) The problem of routing packets through mobile radio networks remains an open and intensely researched problem; there are already beginnings made in the analysis of networks, where the rate of topological change is neither "too fast" nor "too slow." This is an interesting situation in which adaptive and distributed algorithms are currently being investigated.

(2) Most studies of routing in mobile networks ignore the possibility of including physical and media access control layer issues in the design of routing protocols. A notable exception to this is the work of Pursley and Russell [98, 102, 103]. However, these studies are simulation-based. Consequently, there is a need for analytical solutions to routing problems in mobile packet radio networks that reflect the interplay among the physical, media access, and network layers.

(3) Recently, there has been a trend in the literature to combine the determination of network connectivity with the process of routing packets. An example is the recent paper by Corson and Ephremides [96], where a path from a source to destination node also implies the formation and activation of links constituting that path. This is in variance to earlier approaches in the literature [1] that have relied on the use of a specific network organization algorithm.

(4) Finally, there are few global performance measures for comparing the evaluation of different packet radio networks. We conjecture that this problem arises since modeling the different issues in such networks is complex. This modeling complexity has lead to analysis in the literature under various simplifying assumptions, making a realistic comparison of approaches difficult.

References

[1] A. Ephremides, J. E. Wieselthier, and D. J. Baker, "A design concept for reliable mobile radio networks with frequency hopping signaling," *Proceedings of the IEEE*, vol. 75, pp. 56–73, January 1987.

[2] J. E. Wieselthier, D. J. Baker, and A. Ephremides, "Survey of problems in the design of an HF Intra Task Force communication network," Tech. Rep. 8501, NRL, October 1981.

[3] D. J. Baker, J. E. Wieselthier, A. Ephremides, and D. N. McGregor, "Resistance to HF jamming interference in mobile radio networks by an adaptive distributed reconfiguration technique," Tech. Rep. 8834, NRL, August 1984.

[4] D. J. Baker, A. Ephremides, and J. E. Wieselthier, "An architecture for the HF Intra Task Force (ITF) Communication Network," Tech. Rep. 8638, NRL, December 1982.

[5] D. J. Baker and A. Ephremides, "The architectural organization of a mobile radio network via a distributed algorithm," *IEEE Transactions on Communications*, vol. COM-29, pp. 1694–1701, November 1981.

[6] D. J. Baker, A. Ephremides, and J. A. Flynn, "The design and simulation of a mobile radio network with distributed control," *IEEE Journal on Selected Areas in Communications*, vol. SAC-2, pp. 226–237, January 1984.

[7] F. A. Tobagi and L. Kleinrock, "Packet switching in radio channels: Part II-The hidden terminal problem in carrier sense multiple access and the busy tone solution," *IEEE Transactions on Communications*, vol. Com-23, pp. 1417–1433, December 1975.

[8] Proceedings of the IEEE, *Special issue on packet radio networks*, vol. 75, January 1987.

[9] R. C. Dixon, *Spread Spectrum Systems.* New York: John Wiley, 1976.

[10] J. K. Holmes, *Coherent Spread Spectrum Systems.* New York: John Wiley, 1982.

[11] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt, *Spread Spectrum Communications*, vol. 1-3. Maryland: Computer Science Press, 1985.

[12] IEEE Journal on Selected Areas in Communications, *Special issue on spread spectrum*, vol. 4, May 1992.

[13] B. Sklar, *Digital Communications.* New Jersey: Prentice-Hall, 1988.

[14] F. A. Tobagi, "Modeling and performance analysis of multihop packet radio networks," *Proceedings of the IEEE*, vol. 75, pp. 135–155, January 1987.

[15] N. Abramson, "The ALOHA system-another alternative for computer communications," in *AFIPS Conference Proceedings*, vol. 37, pp. 281–285, FJCC, 1970.

[16] N. Abramson, "Packet switching with satellites," in *AFIPS Conference Proceedings*, vol. 42, June 1973.

[17] N. Abramson, "The throughput of packet broadcast channels," *IEEE Transactions on Communications*, vol. COM-25, pp. 117–128, January 1977.

[18] L. Kleinrock and S. Lam, "Packet-switching in a slotted satellite channel," in *Nat. Computer Conf. AFIPS Conf. Proceedings*, vol. 42, pp. 703–710, 1973.

[19] L. G. Roberts, "ALOHA packet system with and without slots and capture," ASS Note 8 NIC 112390, ARPA Network Information Center, Stanford Res. Inst. Menlo Park, CA, June 1972.

[20] L. G. Roberts, "ALOHA packets system with and without slots and capture," *Computer Communications Rev.*, vol. 5, pp. 28–42, April 1975.

[21] D. H. Davis and S. A. Gronemeyer, "Performance of slotted ALOHA random access with delay capture and randomized time of arrival," *IEEE Transactions on Communications*, vol. COM-28, pp. 703–710, May 1980.

[22] L. Kleinrock and F. A. Tobagi, "Carrier sense multiple access for packet switched radio channels," in *Proceedings IEEE Int. Computer Conference*, vol. 42 (Minneapolis, MN), pp. 21B–1–21B–7, June 1974.

[23] L. Kleinrock and F. A. Tobagi, "Packet switching in radio channels: Part I-Carrier sense multiple access modes and their throughput-delay characteristics," *IEEE Transactions on Communications*, vol. COM-23, pp. 1400–1416, December 1975.

[24] J. M. Brazio and F. A. Tobagi, "Throughput analysis of spread-spectrum multihop packet radio networks," in *Proceedings INFOCOM'85* (Washington DC), March 1985.

[25] P. Spilling and F. A. Tobagi, "Activity signaling and improved hop acknowledgements in packet radio systems," Tech. Rep. 283, SRI-International, Menlo Park, CA, January 1980.

[26] F. A. Tobagi and D. H. Shur, "Performance evaluation of channel access schemes in multihop packet radio networks with regular structure by simulation," Tech. Rep. 85-278, CSL, Stanford University, Stanford, CA, June 1985.

[27] J. M. Brazio, *Throughput analysis of multihop packet radio networks under a general class of channel access protocols and capture modes.* Ph.D. Thesis, Stanford University, Department Electrical Engineering, Stanford University, Stanford, CA, June 1986.

[28] J. I. Capetenakis, "Tree algorithms for the packet broadcast channel," *IEEE Trans. Inform. Theory*, vol. IT-25, pp. 505–515, September 1979.

[29] J. I. Capetenakis, "Generalized TDMA: The multi-accessing tree protocol," *IEEE Trans. on Communications*, vol. COM-27, pp. 1476–1484, October 1979.

[30] J. Hayes, "An adaptive technique for local distribution," *IEEE Trans. on Communications*, vol. COM-26, pp. 1178–1186, August 1978.

[31] B. S. Tsybakov and V. A. Mikhailov, "Free synchronous packet access in a broadcast channel with feedback," *Probl. Peredach. Inform.*, vol. 14, pp. 32–59, October 1978.

[32] R. G. Gallager, "A perspective on multiaccess channels," *IEEE Trans. Inform. Theory*, vol. IT-31, pp. 124–142, March 1985.

[33] B. S. Tsybakov, "Survey of USSR contributions to random access multiple-access communications," *IEEE Trans. Inform. Theory*, vol. IT-31, pp. 143–165, March 1985.

[34] B. Hajek, "Balanced scheduling in a packet synchronized spread spectrum network," in *Proceedings 1983 IEEE INFOCOM*, pp. 56–65, April 1983.

[35] M. J. Post, P. E. Sarachik, and A. S. Kershenbaum, "A 'biased-greedy' algorithm for scheduling multi-hop radio networks," in *Proceedings 19th Annual Conference on Information Sciences and Systems*, pp. 564–572, The Johns Hopkins University, March 1985.

[36] M. J. Post, A. S. Kershenbaum, and P. E. Sarachik, "A distributed evolutionary algorithm for reorganizing network communications," in *Proceedings of MILCOM*, pp. 133–139, MILCOM, October 1985.

[37] J. A. Silvester, "Perfect scheduling in multi-hop broadcast networks," in *Proceedings 6th Int. Conference on Computer Communications* (London, England), September 1982.

[38] D. J. Baker, J. E. Wieselthier, and A. Ephremides, "A channel access protocol for survivable radio networks with frequency hopping spread spectrum signaling," in *Proceedings 22nd Annual Allerton Conference on Communication, Control, and Computing*, pp. 50–59, October 1984.

[39] L. Tassiulas and A. Ephremides, "Jointly optimal routing and scheduling in packet radio networks," *IEEE Transactions on Information Theory*, vol. 38, pp. 165–168, January 1992.

[40] B. Hajek and G. Sasaki, "Link scheduling in polynomial time," *IEEE Transactions on Information Theory*, vol. 34, pp. 910–917, September 1989.

[41] I. Chlamtac and A. Farago, "Making transmission schedules immune to topology changes in multi-hop packet radio networks," *IEEE Transaction on Networking*, vol. 2, pp. 23–29, February 1994.

[42] L. Kleinrock and S. Lam, "Packet-switching in a multiaccess broadcast channel: Performance evaluation," *IEEE Transactions on Communications*, vol. COM-23, pp. 703–710, April 1975.

[43] D. Raychauduri, "Performance analysis of random access packet switched code division multiple access systems," *IEEE Transactions on Communications*, vol. COM-29, pp. 895–901, June 1981.

[44] M. Musser and J. Daigle, "Throughput analysis of an asynchronous code division multiple access (CDMA) system," in *Proceedings ICC 82* (Philadelphia, PA), June 1982.

[45] M. B. Pursley, "Throughput of frequency-hopped spread spectrum communications for packet radio networks," in *Proceedings 1983 CISS* (The Johns Hopkins University, Baltimore, MD), March 1983.

[46] L. Kleinrock, *Queueing Systems*, vol. 2. New York: John Wiley, 1976.

[47] I. Gitman, "On the capacity of slotted ALOHA networks and some design problems," *IEEE Transactions on Communications*, vol. COM-23, pp. 305–317, March 1975.

[48] Y. Yemini, "On channel sharing in discrete-time, multi-access broadcast communication," Tech. Rep. UCLA-ENG-8061, Computer Science Department, University of California, Los Angeles, CA, September 1980.

[49] R. R. Boorstyn and A. Kershenbaum, "Throughput analysis of multihop packet radio networks," in *Proceedings ICC 80* (Seattle, WA), June 1980.

[50] A. Kershenbaum and R. Boorstyn, "Evaluation of throughput in multihop packet radio networks with complex topologies," in *Proceedings in INFOCOM 84* (San Francisco, CA), pp. 330–335, April 1984.

[51] F. A. Tobagi and J. M. Brazio, "Throughput analysis of multihop packet radio network under various channel access schemes," in *Proceedings INFOCOM 83* (San Diego, CA), April 1983.

[52] W. C. N. Chen, *Analysis of busy-tone multiple access protocols for multi-hop packet radio networks.* Ph.D. Thesis, Polytechnic Institute of New York, NY, June 1983.

[53] J. M. Brazio and F. A. Tobagi, "Theoretical results on the throughput analysis of multihop packet radio networks," in *Proceedings ICC'84* (Amsterdam, The Netherlands), May 1984.

[54] M. S. Chen and R. Boorstyn, "Analysis of multihop packet radio networks with receiver directed CDMA," in *Allerton Conference*, October 1984.

[55] M. S. Chen and R. Boorstyn, "Throughput analysis of CDMA multihop packet radio networks in the presence of noise," in *Proceedings INFOCOM 85* (Washington DC), April 1985.

[56] P. Sen, "Local markov models for multihop packet radio networks: CDMA," in *Proceedings IEEE ICC'86* (Toronto, Ont., Canada), June 1986.

[57] Y. Yemini, "A statistical mechanics of distributed resource mechanism sharing," in *Proceedings INFOCOM'83* (San Diego, CA), April 1983.

[58] L. Kleinrock and J. A. Silvester, "Spatial reuse in multihop packet radio networks," *Proceedings of the IEEE*, vol. 75, pp. 156–167, January 1987.

[59] J. A. Silvester and L. Kleinrock, "On the capacity of multihop slotted ALOHA networks with regular structure," *IEEE Transactions on Communications*, vol. COM-31, pp. 974–982, August 1983.

[60] A. Ephremides, "The capture effect in spread spectrum multiaccess communications," in *Proceedings Princeton Conference*, March 1982.

[61] A. Ephremides, *Secure digital communications*, ch. 5, CISM Summer School, Udine, 1982.

[62] F. A. Tobagi and L. Kleinrock, "Packet switching in radio channels: Part IV: Stability considerations and dynamic control in carrier sense multiple access," *IEEE Transactions on Communications*, vol. COM-25, pp. 1103–1120, October 1977.

[63] F. A. Tobagi, "Distribution of packet delay and interdeparture time in slotted ALOHA and CSMA channels," *Journal Assoc. Comput. Mach.*, vol. 29, pp. 907–927, October 1982.

[64] S. Lam and L. Kleinrock, "Packet-switching in a multiaccess broadcast channel: Dynamic control procedures," *IEEE Transactions on Communications*, vol. COM-23, pp. 891–904, September 1975.

[65] F. A. Tobagi and L. Kleinrock, "On the analysis and simulation of buffered packet radio systems," in *Proceedings 9th Int. Conf. on System Science* (University of Hawaii, Honolulu), January 1976.

[66] L. Kleinrock and Y. Yemini, "Interfering queueing processes in packet-switched broadcast communication," in *IFIP Cong.* (Tokyo, Japan), 1980.

[67] M. Sidi and A. Segall, "Two interfering queues in packet radio networks," *IEEE Transactions on Communications*, vol. COM-31, January 1983.

[68] M. Sidi and A. Segall, "An acknowledged-based scheme in a two-node packet radio network," *IEEE Transactions on Communications*, vol. COM-32, pp. 741–744, June 1984.

[69] M. Sidi and A. Segall, "A three-node packet radio network," in *Proceedings INFOCOM 83*, pp. 222–228, April 1983.

[70] P. Nain, "Analysis of a two-node ALOHA network with infinite capacity buffers," in *Proc. Int. Seminar Comp. Networking and Perf. Eval.* (Tokyo, Japan), pp. 2.2.1–2.2.15, 1985.

[71] G. Fayolle and R. Iasnogorodsky, "Two-coupled processors: The reduction to a Riemman-Hilbert problem," *Z. Wahrscheinlichkeitstheorie*, vol. 47, pp. 325–351, 1979.

[72] T. N. Saadawi and A. Ephremides, "Analysis, stability, and optimization of slotted ALOHA with a finite number of buffered users," *IEEE Transactions on Automat. Contr.*, vol. AC-26, pp. 680–689, June 1981.

[73] F. A. Tobagi, "Performance analysis of packet radio communication systems," in *Proc. IEEE Nat. Telecommunication Conf.* (Los Angeles, CA), pp. 12:6–1–12:6–7, December 1977.

[74] F. A. Tobagi, "Analysis of slotted ALOHA in a centralized two-hop packet radio network," in *Proc. 7th IEEE Computer Society Int. Conf.* (Washington DC), September 1978.

[75] F. A. Tobagi, "Analysis of a two-hop centralized packet radio network-Part I: Slotted ALOHA," *IEEE Transactions on Communications*, vol. COM-28, pp. 196–207, February 1980.

[76] F. A. Tobagi, "Analysis of a two-hop centralized packet radio network-Part II: Carrier sense multiple access," *IEEE Transactions on Communications*, vol. COM-28, pp. 208–216, February 1980.

[77] A. Fukuda and Y. Muramatsu, "Performance analysis of packet radio networks with repeaters," *Trans. IECE Japan*, vol. J64-B, December 1981.

[78] R. Roy and T. Saadawi, "Analysis of multihop packet radio networks-Carrier sense multiple access with busy tone and collision detection (CSMA/BT-CD)," in *Proc. INFOCOM 84* (San Francisco, CA), April 1984.

[79] H. Takagi and L. Kleinrock, "Throughput-delay characteristics of some slotted-ALOHA multihop packet radio networks," *IEEE Transactions on Communications*, vol. COM-33, pp. 1200–1207, November 1985.

[80] B. M. Leiner, "A simple model for computation of packet radio network communication performance," *IEEE Transactions on Communications*, vol. 28, pp. 2020–2023, December 1980.

[81] I. Lee and J. A. Silvester, "An iterative scheme for performance modeling of slotted ALOHA packet radio networks," in *Proc. ICC*, pp. 6G.1.1–6G.1.5, June 1982.

[82] J. A. Silvester and I. Lee, "Performance modeling of buffered CSMA - an iterative approach," in *Conf. Rec. GLOBECOM* (Miami, FL), pp. F1.6.1–F1.6.5, November 1982.

[83] D. Bertsekas and R. Gallager, *Data Networks.* Englewood Cliffs, NJ: Prentice Hall, Inc., 1987.

[84] D. Torrieri, "Algorithms for finding an optimal set of short disjoint paths in a communication network," *IEEE Trans. on Communications*, vol. 40, pp. 1698–1702, November 1992.

[85] M. Schwartz, *Telecommunication Networks.* New York: Addison-Wesley, 1987.

[86] A. Ephremides and S. Verdu, "Control and optimization methods in communication network problems," *IEEE Trans. on Automatic Control*, vol. 34, pp. 930–941, September 1989.

[87] M. L. Bates, *"A simulated performance study of some distributed routing algorithms for mobile radio networks,"* Master's Thesis, University of Maryland, College Park, 1986.

[88] J. Jubin and J. Tornow, "The DARPA packet radio network," *Proceedings of the IEEE*, vol. 75, pp. 21–32, January 1987.

[89] P. Sass, "Adaptive spread spectrum network research-eccm and low probability of intercept for radio networks," Tech. Rep. Res. Dev. CECOM-TR-84-4, U.S. Army CECOM, 1984.

[90] J. A. Stevens, "Least interference routing," in *Proc. Tactical Commun. Conf.*, pp. 42–51, May 1988.

[91] J. A. Stevens, *Spatial reuse through dynamic power and routing control in common-channel random-access packet radio networks.* Ph.D. Thesis, University of Texas, Dallas, 1988.

[92] J. Westcott and J. Jubin, "A distributed routing design for a broadcast environment," in *1982 IEEE Military Communications Conference Rec.*, vol. 3, pp. 10.4.1–5, October 1982.

[93] J. Jubin, "Current packet radio network protocols," *IEEE INFOCOMM Proc.*, pp. 86–92, March 1985.

[94] B. Awerbuch, A. Bar-Noy, and M. Gopal, "Approximate distributed Bellman-Ford algorithms," *IEEE Transactions on Communications*, vol. COM-42, pp. 2515–2517, August 1994.

[95] E. Gafni and D. Bertsekas, "Distributed algorithms for generating loop-free routes in networks with frequently changing topology," *IEEE Transactions on Communications*, January 1981.

[96] M. S. Corson and A. Ephremides, "A distributed routing algorithm for mobile wireless networks," *WIRELESS NETWORKS*, vol. 1, January 1995.

[97] P. A. Humblet, "Another adaptive distributed shortest path algorithm," *IEEE Trans. on Communications*, vol. 39, pp. 995–1003, June 1991.

[98] M. B. Pursley and H. B. Russell, "Routing in frequency-hop packet radio networks with partial-band jamming," *IEEE Transactions on Communications*, vol. 41, pp. 1117–1124, July 1993.

[99] J. R. McChesney and M. B. Pursley, "Channel access/multiple access performance for SINCGARS packet switched radio network," in *Proceedings Tactical Commun. Conf.*, vol. 1, pp. 7–10, April 1986.

[100] M. B. Pursley, "Frequency-hop transmission for satellite packet switching and terrestrial packet radio networks," *IEEE Transactions on Information Theory*, vol. IT-32, pp. 652–667, September 1986.

[101] M. B. Pursley, "Packet error probabilities in frequency-hop radio networks-coping with statistical dependence and noisy side information," *IEEE Global Telecommun. Conf. Rec.*, vol. 1, pp. 165–170, December 1986.

[102] M. B. Pursley and H. B. Russell, "Adaptive forwarding in frequency-hop spread-spectrum packet radio networks with partial-band jamming," *IEEE Transactions on Communications*, vol. 41, pp. 613–620, April 1993.

[103] M. B. Pursley and H. B. Russell, "Network protocols for frequency-hop packet radios with decoder side information," *IEEE Journal on Selected Areas in Communications*, vol. 12, pp. 612–621, May 1994.

[104] M. B. Pursley, "The derivation and use of side information in frequency-hop spread spectrum," *IEICE Trans. Commun. Special Issue Spread Spectrum Techniques and Application*, vol. E76-B, pp. 814–824, August 1993.

[105] J. J. Garcia-Luna-Aceves, "A minimum-hop routing algorithm based on distributed information," *Computer Networks and ISDN Systems*, pp. 367–382, 1989.

[106] J. Behrens and J. J. Garcia-Luna-Aceves, "Distributed, scalable routing based on link-state vectors," *Computer Communications Review*, vol. 24, pp. 136–147, August 1994.

[107] K. Pahlavan and A. H. Levesque, "Wireless data communications," *Proceedings of IEEE*, vol. 82, September 1994.

[108] B. Tuch, "An ISM band spread spectrum local area network: WaveLAN," in *Proc. IEEE Workshop on Wireless LANs*, pp. 103–111, May 1991.

[109] T. Freeburg, "A new technology for high speed wireless local area networks," in *Proc. IEEE Workshop on Wireless LANs*, pp. 127–139, May 1991.

[110] A. Santamaria and F. J. Lopez-Hernandez, *Wireless LAN Systems.* Boston, MA: Artech House, 1994.

[111] D. Schaum, "MSE mobile subscriber equipment," *Army Commun.*, vol. 9, pp. 6–22, 1984.

[112] V. O. K. Li, "Multiple access communications networks," *IEEE Communications Magazine*, vol. 25, pp. 41–48, June 1987.

Intentionally Left Blank

Appendix A: Radio Communication

Intentionally Left Blank

In this appendix, we review the main characteristics of fading radio channels and examine their impact on the design of packet radio networks. We also discuss the common models that are used to account for effects of propagation path loss and multipath propagation.

WAVE PROPAGATION

Radio propagation in indoor and outdoor environments is quite complicated. Consequently, it has received much attention in the literature [1]. In radio networks, the signal arriving at the receiver is subject to (a) free-space transmissions, and (b) transmissions through objects, reflections, and diffractions. The radio waves travel from transmitter to receiver via many paths, with various received signal strengths. The transit time of the signal along any of the various paths is proportional to the length of the path. The strength of each path is determined by the attenuation caused as the signal passes through, reflects from, or diffracts around objects along the path.

For indoor and outdoor mobile applications, the commonly used mathematical model for a multipath channel is the one suggested by Turin [2] for urban radio propagation. In this model, the impulse response of the channel is given by

$$h(t,\tau) = \sum_{k=1}^{L} \beta_k \delta(t-\tau_k) e^{\theta_k}, \tag{A.1}$$

where $\beta_k, \tau_k, \theta_k$ represent the magnitude, excess delay, and phase of the arriving paths, respectively.

Radio propagation is generally characterized by three parameters: the root-mean-square (rms) multipath delay spread, the gradient of the distance-power relation, and the Doppler spread. The normalized and averaged received power, as a function of delay, is referred to as the *delay-power spectrum* [3]. The *rms multipath delay spread* is the square root of the second central moment of the delay-power spectrum. With the previously mentioned mathematical

model, the rms multipath delay spread is given by

$$\tau_{rms} = \left[\frac{\sum_{k=1}^{L}(\tau_k - \bar{\tau})^2\beta_k^2}{\sum_{k=1}^{L}\beta_k^2}\right]^{\frac{1}{2}}, \tag{A.2}$$

where

$$\bar{\tau} = \frac{\sum_{k=1}^{L}\tau_k\beta_k^2}{\sum_{k=1}^{L}\beta_k^2} \tag{A.3}$$

is the *mean excess delay*. While in most indoor radio networks, the rms multipath delay spread measured at maximum distances of 100 m is below 100 ns, in outdoor areas, it is less than 10 μs at distances up to a few kilometers. As a rule, the multipath spreads in urban canyons and hilly terrains are more than in flat residential areas. Further statistics and measurements are available for a variety of situations in the literature [2, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17].

Multipath affects the average received signal power and, consequently, causes the received power to fluctuate statistically as a node moves around, or as people move around close to the receiver or transmitter. The average received signal power, as a function of the path amplitudes, is given by

$$P_r = \sum_{k=1}^{L}|\beta_k|^2. \tag{A.4}$$

It is proportional to the inverse of the distance between receiver and transmitter, raised to a certain power. This power factor is called the *distance-power gradient*, which multiplied by ten gives the power loss in decibels per decade of increase in the distance. In free-space radio propagation, the distance-power gradient is 2. This means the received power decays with the inverse of the square of the distance between receiver and transmitter, or the power decays at the rate of 20 dB per decade or distance. For indoor and urban radio channels, the distance-power relationship changes according to many factors, including building and street layouts, construction material, and density and height of buildings in the area.

The fluctuation of the average received power is caused by shadowing and appropriately referred to as *shadow fading*. The phase differences in the arriving paths cause the amplitude

of the signal to have a fast-changing component. This fluctuation is referred to as *multipath fading*. Two different models have been developed for line-of-sight (LOS) and obstructed LOS (OLOS) communications. For LOS communications, the path amplitude variations are modeled with Rician or log-normal distributions; in OLOS communications, they are modeled with a Rayleigh distribution. For results of measurements in different environments at different frequencies see references [10, 11, 12, 13, 17, 18, 19, 20, 21, 22, 23, 24, 25].

When a receiver and a transmitter are in relative motion with velocity v_m, the received carrier frequency f_d will differ from the transmitted carrier frequency f_c. This shift in frequency is referred to as the *Doppler shift* and is given by

$$f_d = \frac{v_m}{C} f_c, \tag{A.5}$$

where C is the velocity of radio wave propagation. Whether the transmitter is moving toward or away from the receiver will determine if the Doppler frequency shift is positive or negative. For a mobile terminal moving at a speed of 60 mph relative to the receiver, the Doppler shift is 120 Hz.

Generally, the received signal arrives along several reflected paths. The velocity of movement in the direction of each arriving path is usually different from one path to another. Consequently, a transmitted sinusoidal signal is not subject to a simple Doppler shift, but rather is received as a spectrum. This spectrum is referred to as the *Doppler spectrum.* The effect is viewed as a spreading of the transmitted signal frequency and is referred to as the *Doppler spread* of the channel. Doppler spread can also occur with a fixed transmitter and receiver: when an object moves within the propagation path, it produces time varying multipath characteristics. In a radio network, as the terminals move about (or objects move around the terminals), the received signal fluctuates. These fluctuations in the observed signal affect the width of the Doppler spread in the frequency domain. Narrow-band measurements of the Doppler spread can be found in Howard and Pahlavan, Bultitude, and Rappaport and Hawbaker [14, 21, 26], while short time variations for wideband indoor radio propagation can be found in Ganesh and Pahlavan [27, 28].

The design of a packet radio network is influenced by the operational characteristics of the radio frequency (RF) band [29]. While considerations of bandwidth determine the lowest frequencies allowed for a packet radio system, propagation path loss and the associated RF power generation requirement determine the highest frequencies allowable.

The impact of bandwidth on the lowest desirable RF is subtle. If the ratio of RF bandwidth to RF center frequency is much larger than about 0.3, practical, cost-effective radio equipment is difficult to build. Hence, the range of acceptable RF center frequencies is bounded below. From an implementation viewpoint, the RF center frequency should be in the lower high-frequency (HF) band extending from 3 MHz to 30 MHz. While propagation in the HF band can provide long-distance communication due to sky-wave reflections, the signal also experiences multipath spreading of the signal. Thus, there is a limitation on the data-rate of signals that can be used. In the very high-frequency (VHF) band from 30 MHz to 300 MHz, multipath spreading is usually reduced to a few microseconds as compared to the millisecond spreads present in the HF band. In the VHF band, data rates on the order of 100 kilobits can be achieved. However, distortion and multipath fading are still problems at VHF, particularly for mobile terminals or terminals that do not operate with radio LOS. These difficulties can be overcome by spread-spectrum signaling.

Propagation path loss establishes an upper bound on the usable radio frequencies for packet radio networks. If the operating frequency is raised above 10 GHz, losses due to absorption by rain and atmosphere rapidly increase, and the radio range is reduced. Consequently, packet radio networks must rely on closely spaced relays to provide adequate area coverage at these frequencies. A resulting concern is the cost and overhead of providing a dense relay population. However, in a ground-based packet radio system 10 GHz is a practical upper bound for useful RF. As a result, desirable RF bands for a packet radio network are the upper VHF band, the ultrahigh-frequency (UHF) band from 300 MHz to 3 GHz, and the

lower part of the superhigh-frequency (SHF) band from 3 GHz to 30 GHz.

Since VHF and UHF bands are heavily allocated, another important consideration is the authorization of packet radio transmissions. Spread-spectrum signaling could allow for the coexistence of a packet radio system with existing users within a frequency band.

References

[1] K. Pahlavan and A. H. Levesque, "Wireless data communications," *Proceedings of IEEE*, vol. 82, September 1994.

[2] G. L. Turin, F. D. Clapp, T. L. Johnston, S. B. Fine, and D. Lavry, "A statistical model of urban multipath propagation," *IEEE Transactions on Vehicular Technology*, vol. VT-21, pp. 1–9, February 1972.

[3] P. A. Bello, "A troposcatter channel model," *IEEE Transactions on Communication Technology*, vol. COM-17, pp. 130–137, April 1969.

[4] D. M. J. Devasirvatham, "Time delay spread measurements of wideband radio systems within a building," *Electronic Letters*, vol. 20, pp. 949–950, 1984.

[5] D. M. J. Devasirvatham, "Time delay spread measurement of 850 MHz radio waves in building environment," *GLOBECOM*, pp. 32.1.1–32.1.5, 1985.

[6] D. M. J. Devasirvatham, "Time delay spread and signal level measurements of 850 MHz radio waves in building environment," *IEEE Transactions on Antennas Propagation*, pp. 1300–1305, November 1986.

[7] D. M. J. Devasirvatham, "A comparison of time delay spread and signal level measurements within two dissimilar office buildings," *IEEE Transactions on Antennas Propagation*, pp. 319–324, March 1987.

[8] D. M. J. Devasirvatham, R. R. Murray, and C. Banerjee, "Time delay spread measurements at 850 MHz and 1.7 GHz inside a metropolitan office building," *IEE Electronic Letters*, pp. 194–196, February 1989.

[9] R. J. C. Bultitude, S. A. Mahmmoud, and W. A. Sullivan, "A comparison of indoor radio propagation characteristics at 910 MHz and 1.75 GHz," *IEEE Journal on Selected Areas in Communications*, vol. 7, pp. 20–30, January 1989.

[10] T. S. Rappaport and C. D. McGillem, "UHF fading in factories," *IEEE Journal on Selected Areas in Communications*, vol. 7, pp. 40–48, January 1989.

[11] T. S. Rappaport, "Characterization of UHF multipath radio channels in factory buildings," *IEEE Transactions on Antennas Propagation*, pp. 1058–1069, August 1989.

[12] K. Pahlavan, R. Ganesh, and T. Hotaling, "Multipath propagation measurements on manufacturing floors at 910 MHz," *Electronic Letters*, February 1989.

[13] K. Pahlavan and S. J. Howard, "Frequency domain measurements of the indoor radio channel," *Electronic Letters*, November 1989.

[14] S. J. Howard and K. Pahlavan, "Measurement and analysis of the indoor radio channel in the frequency domain," *IEEE Transactions on Instrum. Meas.*, October 1990.

[15] S. J. Howard, *Frequency domain characteristics and autoregressive modeling of the indoor radio channel.* Ph.D. Thesis, Worcester Polytechnical Institute, May 1991.

[16] R. Ganesh and K. Pahlavan, "Modeling of the indoor radio channel," in *Proceedings Inst. Elec. Eng.-I*, June 1991.

[17] R. Ganesh and K. Pahlavan, "Statistical characterization of a partitioned indoor radio channel," in *Proceedings Inst. Elec. Eng.-I, Communication, Speech and Vision*, November 1992.

[18] S. E. Alexander, "Radio propagation within buildings at 900 MHz," *IEE Electronic Letters*, pp. 913–914, October 1982.

[19] S. E. Alexander, "Characterizing buildings for propagation at 900 MHz," *IEE Electronic Letters*, p. 860, September 1983.

[20] A. J. Motley and J. M. P. Keenan, "Personal communication radio coverage in buildings at 900 MHz and 1700 MHz," *IEE Electronic Letters*, pp. 763–764, June 1988.

[21] R. J. C. Bultitude, "Measurement, characterization and modeling of indoor 800/900 MHz radio channels for digital communications," *IEEE Communications Magazine*, vol. 25, pp. 5–12, June 1987.

[22] A. R. Tharek and J. P. McGeehan, "Indoor radio propagation and bit error rate measurements at 60 GHz using phase-locked oscillators," in *Proceedings 38th Vehicular Technology Conference* (Philadelphia, PA), pp. 127–133, 1988.

[23] A. M. D. Turkamani and A. F. Toleda, "Radio transmission at 1800 MHz into and within multistory buildings," in *Proc. Inst. Elec. Eng. I*, pp. 577–584, December 1991.

[24] H. Zhoghloul, G. Morrison, and M. Fottouche, "Frequency response and path loss measurements of indoor channel," in *Proc. Inst. Elec. Eng.-I*, vol. 12, June 1991.

[25] S. Y. Seidel and T. S. Rappaport, "914 MHz path loss prediction models for wireless communications in multifloored buildings," *IEEE Transactions on Antennas Propagation*, pp. 207–217, Feb 1992.

[26] T. S. Rappaport and D. A. Hawbaker, "A ray tracing technique to predict path loss and delay spread inside buildings," in *Proceedings IEEE GLOBECOM 92*, pp. 649–653, December 1992.

[27] R. Ganesh and K. Pahlavan, "Effects of local traffic and local movements on the multipath characteristics of the indoor radio channel," *Electronic Letters*, June 1990.

[28] R. Ganesh and K. Pahlavan, "Statistics of short time and spatial variations measured in wideband indoor radio channels," in *Proceedings Inst. Elec. Eng.-H, Microwave, Antennas Propagation*, November 1993.

[29] R. E. Kahn, S. A. Gronmeyer, J. Burchfiel, and R. C. Kunzelman, "Advances in packet radio technology," *Proceedings of the IEEE*, vol. 66, pp. 1468–1496, November 1978.

Bibliography

[1] A. Kershenbaum, R. R. Boorstyn, and M. S. Chen. An algorithm for evaluation of throughput in multihop packet radio networks with complex topologies. *IEEE Journal on Selected Areas in Communications*, SAC-5:1003–1012, July 1987.

[2] B. M. Leiner, D. L. Nielson, and F. A. Tobagi. Issues in packet radio network design. *Proceedings of the IEEE*, 75:6–20, January 1987.

[3] M. B. Pursley. The role of spread-spectrum in packet radio networks. *Proceedings of the IEEE*, 75(1):116–134, January 1987.

[4] N. Schacham and P. J. B. King. Architectures and performance of multichannel multihop packet broadcast networks. *IEEE Journal on Selected Areas in Communications*, SAC-5:1013–1026, July 1987.

[5] E. S. Sousa and J. A. Silvester. Optimum transmission ranges in a direct-sequence spread-spectrum multi-hop packet radio network. *IEEE Journal on Selected Areas in Communications*, 8:762–771, June 1990.

[6] H. Takagi and L. Kleinrock. Optimal transmission ranges for randomly distributed packet radio terminals. *IEEE Transactions on Communications*, COM-32:246–257, March 1984.

[7] F. A. Tobagi. Multiaccess protocols in packet communication systems. *IEEE Transactions on Communications*, COM-28:468–488, April 1980.

[8] F. A. Tobagi, M. Gerla, R. W. Peebles, and E. G. Manning. Modeling and measurement techniques in packet communication networks. *Proceedings of the IEEE*, 66(11):1423–1447, November 1978.

[9] B. S. Tsybakov and V. L. Bakirov. Packet transmission in radio networks. *Problemy Peredachi Informatsii*, 21:80–101, January-March 1985.

NO. OF COPIES	ORGANIZATION
2	DEFENSE TECHNICAL INFORMATION CENTER DTIC DDA 8725 JOHN J KINGMAN RD STE 0944 FT BELVOIR VA 22060-6218
1	HQDA DAMO FDQ DENNIS SCHMIDT 400 ARMY PENTAGON WASHINGTON DC 20310-0460
1	DPTY ASSIST SCY FOR R&T SARD TT F MILTON RM 3EA79 THE PENTAGON WASHINGTON DC 20310-0103
1	OSD OUSD(A&T)/ODDDR&E(R) J LUPO THE PENTAGON WASHINGTON DC 20301-7100
1	CECOM SP & TRRSTRL COMMCTN DIV AMSEL RD ST MC M H SOICHER FT MONMOUTH NJ 07703-5203
1	PRIN DPTY FOR TCHNLGY HQ US ARMY MATCOM AMCDCG T M FISETTE 5001 EISENHOWER AVE ALEXANDRIA VA 22333-0001
1	PRIN DPTY FOR ACQUSTN HQS US ARMY MATCOM AMCDCG A D ADAMS 5001 EISENHOWER AVE ALEXANDRIA VA 22333-0001
1	DPTY CG FOR RDE HQS US ARMY MATCOM AMCRD BG BEAUCHAMP 5001 EISENHOWER AVE ALEXANDRIA VA 22333-0001

NO. OF COPIES	ORGANIZATION
1	INST FOR ADVNCD TCHNLGY THE UNIV OF TEXAS AT AUSTIN PO BOX 202797 AUSTIN TX 78720-2797
1	USAASA MOAS AI W PARRON 9325 GUNSTON RD STE N319 FT BELVOIR VA 22060-5582
1	CECOM PM GPS COL S YOUNG FT MONMOUTH NJ 07703
1	GPS JOINT PROG OFC DIR COL J CLAY 2435 VELA WAY STE 1613 LOS ANGELES AFB CA 90245-5500
1	ELECTRONIC SYS DIV DIR CECOM RDEC J NIEMELA FT MONMOUTH NJ 07703
3	DARPA L STOTTS J PENNELLA B KASPAR 3701 N FAIRFAX DR ARLINGTON VA 22203-1714
1	USAF SMC/CED DMA/JPO M ISON 2435 VELA WAY STE 1613 LOS ANGELES AFB CA 90245-5500
1	US MILITARY ACADEMY MATH SCI CTR OF EXCELLENCE DEPT OF MATHEMATICAL SCI MDN A MAJ DON ENGEN THAYER HALL WEST POINT NY 10996-1786
1	DIRECTOR US ARMY RESEARCH LAB AMSRL CS AL TP 2800 POWDER MILL RD ADELPHI MD 20783-1145

NO. OF COPIES	ORGANIZATION
1	DIRECTOR US ARMY RESEARCH LAB AMSRL CS AL TA 2800 POWDER MILL RD ADELPHI MD 20783-1145
3	DIRECTOR US ARMY RESEARCH LAB AMSRL CI LL 2800 POWDER MILL RD ADELPHI MD 20783-1145
	ABERDEEN PROVING GROUND
4	DIR USARL AMSRL CI LP (305)

NO. OF COPIES	ORGANIZATION
1	DIRECTOR US ARMY RESEARCH OFC DR J FREEBERSEYSER PO BOX 12211 RESEARCH TRIANGLE PARK NC 22709-2211
1	COMMANDANT US MIL ACADEMY DEPT OF ELECTRL ENGRG COL W LANE WEST POINT NY 10996
2	COMMANDANT US MIL ACADEMY MATHEMATICAL SCIENCES CTR OF EXCELLENCE DR D WILKERSON MAJ D ENGEN WEST POINT NY 10996
1	COMMANDANT US AIR FORCE ACADEMY COLORADO SPRINGS CO 80840
1	DIRECTOR NAVAL RSRCH LAB CODE 7521 DR J E WIESELTHIER WASHINGTON DC 20375-5000
2	COMMANDER US ARMY CECOM AMSEL RD ST P SASI DR C GRAFF FT MONMOUTH NJ 07703
1	NORTH CAROLINA STATE UNIV DEPT OF ELECTRL & COMPUTER ENGRG B L HUGHES RALEIGH NC 27695-7911
1	MORGAN STATE UNIV DEPT OF ELECTRL ENGRG P MACK BALTIMORE MD 21212

NO. OF COPIES	ORGANIZATION
1	UNIV OF ILLINOIS COORDINATED SCIENCE LAB U MADHOW URBANA IL 61801
1	CLEMSON UNIV HOLCOM PROF OF ELECTRL AND COMPUTER ENGRG M J PURSLEY 102 RIGGS HALL CLEMSON SC 29634
1	UNIV OF TEXAS DIV OF ENGRG S ROY 6900 NORTH LOOP 1604 WEST SAN ANTONIO TX 78249-0665
2	MA INSTITUTE OF TECH DEPT OF ELECTRL ENGRG AND COMPUTER SCIENCE R GALLAGER G WORNELL CAMBRIDGE MA 02139-4307
4	UNIV OF DE DEPT OF COMPUTER & INFO SCIENCES A SETHI P AMER T SAYDAM E LLOYD NEWARK DE 19716
3	UNIV OF DE DEPT OF ELECTRL & COMPUTER ENGRG G ARCE C BONCELET D MILLS NEWARK DE 19716
3	THE UNIV OF MD AT COLLEGE PARK DEPT OF ELECTRL ENGRG A EPHREMIDES C SILIO JR L TASSIULAS COLLEGE PARK MD 20742

NO. OF COPIES	ORGANIZATION
1	THE UNIV OF MD AT COLLEGE PARK INSTITUTE FOR SYS RSRCH DR M S CORSON COLLEGE PARK MD 20742
1	HOWARD UNIV SCHOOL OF ENGRG DEPT OF SYS & COMPUTER SCIENCE J TRIMBLE 2300 6 ST NW WASHINGTON DC 20059
1	TEXAS A&M UNIV DEPT OF ELECTRL ENGRG C CEORGHIADES COLLEGE STATION TX 77843
10	ROCKWELL SEMICONDUCTOR SYS SENIOR ENGRG (R&D) DR R MURALI 9868 SCRANTON RD SAN DIEGO CA 92121-3707
10	THE JOHNS HOPKINS UNIV DEPT OF ELECTRL & COMPUTER ENGRG GWC WHITING SCHOOL OF ENGRG M SUBBARAO BALTIMORE MD 21218
5	MOTOROLA SPACE & SYS TECH GRP M ENNIS B RIVERA (ARL) C TODD M E HUMPHREY S ENSERINK 8201 E MCDOWELL RD SCOTTSDALE AZ 85252-1417
1	BELLCORE MCC-1C121B W CHEN 445 SOUTH ST MORRISTOWN NJ 07960

NO. OF COPIES	ORGANIZATION
2	GEORGIA INST OF TECH AMSRL IS TA B RIVERA DR G RACINE 115 O'KEEFE BLDG ATLANTA GA 30332
2	UNIV OF MIAMI DEPT OF ELECTRL & COMPUTER ENGRG T YOUNG M TAPIA CORAL GABLES FL 33124
2	FLORIDA INTL UNIV DEPT ELECTRL & COMPUTER ENGRG A MALEK W V SUBBARAO UNIVERSITY PARK MIAMI FL 33199
1	TEXAS A&M UNIV ELECTRL ENGRG DEPT C GEORGHIADES COLLEGE STATION TX 77843-3128
1	US NAVAL ACADEMY WEAPONS & SYS ENGRG DEPT R DEMOYER 121 BLAKE RD ANNAPOLIS MD 21402-5000
1	COMMANDANT US NAVAL ACADEMY ANNAPOLIS MD 21404

NO. OF COPIES	ORGANIZATION
	ABERDEEN PROVING GROUND
28	DIR, USARL AMSRL IS (ALC) DR J GANTT DR J CHANDRA DR P EMMERMAN R SLIFE AMSRL IS T (ALC) DR J GOWENS AMSRL IS CB (ALC) L TOKARCIK AMSRL IS TA (ALC) DR B SADLER DR D TORRIERI DR J BRAND G CIRINCIONE H HARRELSON A MARK AMSRL IS CI B D BROOME A BRODEEN D GWYN LTC R HAMMELL DR R HELFMAN R C KASTE AMSRL IS TP DR S CHAMBERLAIN G HARTWIG H CATON F BRUNDICK M LOPEZ C SARAFIDES AMSRL IS TA DR A B COOPER M MARKOWSKI L MARVEL DR C RETTER

NO. OF COPIES	ORGANIZATION
1	THE UNIVERSITY ELECTRICAL ENGINEERING LABORATORIES PROF P G FARRELL MANCHESTER ML3 9PL ENGLAND

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	January 1998	Final, Sep 94 - Jun 95

4. TITLE AND SUBTITLE

A Study of Packet Routing in Mobile Radio Networks

5. FUNDING NUMBERS

C: DAAL03-91-C-0034

6. AUTHOR(S)

Madhavi Subbarao and Ramaswamy Murali

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Department of Electrical and Computer Engineering
The Johns Hopkins University
Baltimore, MD 21218

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAMES(S) AND ADDRESS(ES)

U. S. Army Research Laboratory
ATTN: AMSRL-IS-TA
Aberdeen Proving Ground, MD 21005-5067

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

ARL-CR-337

11. SUPPLEMENTARY NOTES

Task was performed under a Scientific Services Agreement issued by Battelle, Research Triangle Park Office, 200 Park Drive, P.O. Box 12297, Research Triangle Park, NC 27709.

12a. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

This study is concerned with mobile packet radio networks. These networks are of importance in the context of tactical battlefield communications, where decentralized operation and antijam capability are desirable network attributes. The objective of this study is to conduct and document a survey of the known and available results on techniques for routing information through packet radio networks. We focus on issues that reside within the first (lower) three layers of the seven-layer open system interconnection (OSI) network architecture model. Consequently, a greater emphasis is placed on issues, such as network connectivity, media access, and routing. Where available, performance evaluation methods are detailed. Finally, we present examples of commercial, state-of-the-art wireless data networks and discuss some open problems for further study.

14. SUBJECT TERMS

packet routing, mobile packet radio networks, adaptive routing

15. NUMBER OF PAGES

121

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18 298-102

INTENTIONALLY LEFT BLANK.

USER EVALUATION SHEET/CHANGE OF ADDRESS

This Laboratory undertakes a continuing effort to improve the quality of the reports it publishes. Your comments/answers to the items/questions below will aid us in our efforts.

1. ARL Report Number/Author ARL-CR-337 (Subbarao [POC: Cooper]) Date of Report January 1998

2. Date Report Received ______

3. Does this report satisfy a need? (Comment on purpose, related project, or other area of interest for which the report will be used.) ______

4. Specifically, how is the report being used? (Information source, design data, procedure, source of ideas, etc.) ______

5. Has the information in this report led to any quantitative savings as far as man-hours or dollars saved, operating costs avoided, or efficiencies achieved, etc? If so, please elaborate. ______

6. General Comments. What do you think should be changed to improve future reports? (Indicate changes to organization, technical content, format, etc.) ______

CURRENT ADDRESS

Organization

Name E-mail Name

Street or P.O. Box No.

City, State, Zip Code

7. If indicating a Change of Address or Address Correction, please provide the Current or Correct address above and the Old or Incorrect address below.

OLD ADDRESS

Organization

Name

Street or P.O. Box No.

City, State, Zip Code

(Remove this sheet, fold as indicated, tape closed, and mail.)
(DO NOT STAPLE)

DEPARTMENT OF THE ARMY

OFFICIAL BUSINESS

NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES

BUSINESS REPLY MAIL
FIRST CLASS PERMIT NO 0001,APG,MD

POSTAGE WILL BE PAID BY ADDRESSEE

DIRECTOR
US ARMY RESEARCH LABORATORY
ATTN AMSRL IS T
ABERDEEN PROVING GROUND MD 21005-5067